ACADEMIC CURRICULA

POSTGRADUATE DEGREE PROGRAMMES

Master of Technology in Information Security and Cyber Forensics
(Empowered by K7 Computing)

Two Years(Full-Time)

Learning Outcome Based Education

Choice Based Flexible Credit System

Academic Year

2020 - 2021

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Kattankulathur, Chengalpattu District 603203, Tamil Nadu, India

M.Tech in Information Technology
Information Security and Cyber Forensics

1. Department Vision Statement

Stmt - 1	*To develop the skills and knowledge to excel in their professional career in Information Technology and related disciplines.*
Stmt - 2	*To contribute and communicate effectively with the team to grow into leader.*
Stmt - 3	*To practice lifelong learning for continuing professional development.*

2. Department Mission Statement

Stmt - 1	*To develop the ability to use and apply current technical concepts, skills, tools and practices in the core information technology areas.*
Stmt - 2	*To develop the ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based system.*
Stmt - 3	*To develop the ability to effectively integrate IT-based solutions into the user environment.*

3. Program Education Objectives (PEO)

PEO - 1	*To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.*
PEO - 2	*To develop graduates that can plan, implement, and monitor cyber security mechanisms*
PEO - 3	*To ensure the protection of information technology assets.*
PEO - 4	*To enables the students to gain in-depth knowledge in the field of Computer forensics*

4. Consistency of PEO's with Mission of the Department

	Mission Stmt. - 1	Mission Stmt. - 2	Mission Stmt. - 3
PEO - 1	*H*	*H*	*H*
PEO - 2	*H*	*H*	*H*
PEO - 3	*H*	*H*	*M*
PEO - 4	*H*	*H*	*M*

H – High Correlation, M – Medium Correlation, L – Low Correlation

5. Consistency of PEO's with Program Learning Outcomes (PLO)

	Program Learning Outcomes (PLO)														
	1. Disciplinary Knowledge	2. Critical Thinking	3. Problem Solving	4. Analytical Reasoning	5. Research Skills	6. Team Work	7. Scientific Reasoning	8. Reflective Thinking	9. Self-Directed Learning	10. Multicultural Competence	11. Ethical Reasoning	12. Community Engagement	13. ICT Skills	14. Leadership Skills	15. Life Long Learning
PEO - 1	*H*	*H*	*H*	*H*	*M*	*M*	*M*	*H*	*M*	*H*	*M*	*M*	*H*	*M*	*M*
PEO - 2	*H*	*H*	*H*	*H*	*M*	*M*	*M*	*H*	*M*	*M*	*L*	*M*	*H*	*M*	*M*
PEO - 3	*M*	*M*	*M*	*M*	*H*	*M*	*M*	*H*	*L*	*H*	*M*	*M*	*M*	*M*	*H*
PEO - 4	*H*	*H*	*H*	*H*	*M*	*H*	*M*	*H*	*H*	*H*	*H*	*H*	*H*	*L*	*H*

H – High Correlation, M – Medium Correlation, L – Low Correlation

6. Programme Structure (70 Total Credits)

Professional Core Courses (C)

Course Code	Course Title	Hours/ Week L	T	P	C
20MAC504T	Number Theory	3	1	0	4
20ITC552J	Cryptography and Network Security	3	0	2	4
20ITC553J	Malware Analysis	3	0	2	4
20ITC554J	Forensic and Incident Response	3	0	2	4
	Total Learning Credits				16

Skill Enhancement Courses (S)

Course Code	Course Title	Hours/ Week L	T	P	C
20GNS501J	Research Publishing and Presenting Skills	1	0	2	2
20GNS502T	Research Methods in Engineering	3	0	0	3
	Total Learning Credits				5

Project Work, Internship In Industry / Higher Technical Institutions (P)

Course Code	Course Title	Hours/ Week L	T	P	C
20ITP651L	Internship (4-6 weeks during 2nd sem vacation)	-	-	-	4
20ITP652L	Minor Project	0	0	8	
20ITP653L	Project Work Phase I	0	0	12	6
20ITP654L	Project Work Phase II	0	0	32	16
	Total Learning Credits				26

Mandatory Courses (M)

Course Code	Course Title	Hours/ Week L	T	P	C
20PDM501T	Career Advancement Course for Engineers – I	1	0	1	0
20PDM502T	Career Advancement Course for Engineers – II	1	0	1	0
20PDM601T	Career Advancement Course for Engineers – III	1	0	1	0

Professional Elective Courses (E)
(5 Courses)

Course Code	Course Title	Hours/ Week L	T	P	C
20ITE555J	Android Security and Design Internals	3	0	2	4
20ITE556J	Cloud Architectures and Security				
20ITE557J	Security Scripting and Analysis	3	0	2	4
20ITE558J	Principles of Secure Coding				
20ITE559J	Penetration Testing and Vulnerability Assessment	3	0	2	4
20ITE560J	Mobile and Digital Forensics				
20ITE561T	Storage Management and Security	3	1	0	4
20ITE562T	Applied Cryptography				
20ITE642T	Risk Assessment and Security Audit	3	1	0	4
20ITE643T	Cyber Law and Ethics				
	Total Learning Credits				20

Open Elective Courses (O)
(Any 1 Course)

Course Code	Course Title	Hours/ Week L	T	P	C
20MBO601T	Business Analytics	3	0	0	3
20MEO601T	Industrial Safety	3	0	0	3
20MAO501T	Operations Research	3	0	0	3
20MBO602T	Cost Management	3	0	0	3
20NTO601T	Composite Materials	3	0	0	3
20CEO531T	Waste to Energy	3	0	0	3
20ITO601T	MOOC	-	-	-	3
	Total Learning Credits				3

Audit Courses (A)
(Any 2 Courses)

Course Code	Course Title	Hours/ Week L	T	P	C
20CEA531J	Disaster Management	1	0	1	0
20GNA511T	Constitution of India	1	0	0	0
20GNA513J	Value Education	1	0	1	0
20GNA512L	Physical and Mental Health using Yoga	0	0	2	0

7. Implementation Plan

Semester - I

Code	Course Title	Hours/ Week			C
		L	T	P	
20MAC504T	Number Theory	3	1	0	4
20ITC552J	Cryptography and Network Security	3	0	2	4
20ITE555J	Android Security and Design Internals	3	0	2	4
20ITE556J	Cloud Architectures and Security				
20ITE557J	Security Scripting and Analysis	3	0	2	4
20ITE558J	Principles of Secure Coding				
20GNS501J	Research Publishing and Presenting Skills	1	0	2	2
20PDM501T	Career Advancement Course for Engineers – I	1	0	1	0
	Audit Course – 1	1	0	1	0
Total Learning Credits					18

Semester - II

Code	Course Title	Hours/ Week			C
		L	T	P	
20ITC553J	Malware Analysis	3	0	2	4
20ITC554J	Forensic and Incident Response	3	0	2	4
20ITE559J	Penetration Testing and Vulnerability Assessment	3	0	2	4
20ITE560J	Mobile and Digital Forensics				
20ITE561T	Storage Management and Security	3	0	2	4
20ITE562T	Applied Cryptography				
20GNS502T	Research Methods in Engineering	3	0	0	3
20PDM502T	Career Advancement Course for Engineers – II	1	0	1	0
	Audit Course - 2	1	0	1	0
Total Learning Credits					19

Semester - III

Code	Course Title	Hours/ Week			C
		L	T	P	
20ITE642T	Risk Assessment and Security Audit	3	1	0	4
20ITE643T	Cyber Law and Ethics				
	Open Elective	3	0	0	3
20ITO601T	MOOC	-	-	-	
20ITP651L	Internship (4-6 weeks during 2nd Sem vacation)	-	-	-	4
20ITP652L	Minor Project	0	0	8	
20ITP653L	Project Work Phase I	0	0	12	6
20PDM601T	Career Advancement Course for Engineers – III	1	0	1	0
Total Learning Credits					17

Semester - IV

Code	Course Title	Hours/ Week			C
		L	T	P	
20ITP654L	Project Work Phase II	0	0	32	16
Total Learning Credits					16

8. Program Articulation Matrix

Course Code	Course Name	Programme Learning Outcomes														
		Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research Skills	Team Work	Scientific Reasoning	Reflective Thinking	Self-Directed Learning	Multicultural Competence	Ethical Reasoning	Community Engagement	ICT Skills	Leadership Skills	Life Long Learning
20MAC504T	Number Theory	H	H	H	H	H	-	M	M	-	-	-	-	-	-	M
20ITC552J	Cryptography and Network security	M	H	H	M	L	-	M	M	M	L	-	H	-	-	-
20ITC553J	Malware Analysis	M	H	M	M	H	-	-	-	M	L	-	H	-	-	-
20ITC554J	Forensic and Incident Response	H	H	H	H	H	-	H	-	H	-	-	-	-	-	L
20ITE555J	Android Security and Design Internals	M	H	L	M	M	-	-	-	M	L	-	H	-	-	M
20ITE556J	Cloud Architectures and Security	M	H	M	H	L	-	-	-	M	-	-	H	-	-	L
20ITE557J	Security Scripting and Analysis	H	H	H	M	M	-	-	-	M	L	-	-	-	-	M
20ITE558J	Principles of Secure Coding	H	H	H	M	M	-	-	-	M	L	-	-	-	-	M
20ITE559J	Penetration Testing and Vulnerability Assessment	H	M	H	H	M	H	-	M	-	H	M	M	-	M	M
20ITE560J	Mobile and Digital Forensic	H	H	H	H	H	-	H	-	H	-	-	-	-	-	L
20ITE561T	Storage Management and Security	H	H	M	H	M	-	M	M	H	M	-	-	H	-	H
20ITE562T	Applied Cryptography	H	H	H	H	M	-	-	M	-	-	-	-	-	-	H
20ITE642T	Risk Assessment and Security Audit	H	M	M	M	L	M	L	M	-	-	H	L	-	M	M
20ITE643T	Cyber Law and Ethics	H	H	M	H	M	M	M	M	H	M	H	H	H	M	H
20GNS501J	Research Publishing and Presenting Skills															
20GNS502T	Research Methods in Engineering															
20MBO601T	Business Analytics															
20MEO601T	Industrial Safety															
20MAO501T	Operations Research															
20MBO602T	Cost Management															
20NTO601T	Composite Materials															
20CEO531T	Waste to Energy															
20ITO601T	MOOC	M	H	M	H	H	-	-	-	M	L	-	H	-	-	H
20ITP651L	Internship (4-6 weeks)	H	H	H	H	H	H	H	H	H	-	-	-	-	H	H
20ITP653L	Project Work Phase I	H	H	H	H	H		H	H	H	-	-	-	-	-	H
20ITP654L	Project Work Phase II	H	H	H	H	H		H	H	H	-	-	-	-	-	H
20CEA531J	Disaster Management															
20GNA511T	Constitution of India															
20GNA513J	Value Education															
20GNA512L	Physical and Mental Health using Yoga															
20PDM501T	Career Advancement Course for Engineers – I															
20PDM502T	Career Advancement Course for Engineers – II															
20PDM601T	Career Advancement Course for Engineers – III															
	Program Average															

H – High Correlation, M – Medium Correlation, L – Low Correlation

Course Code	20MAC504T	Course Name	NUMBER THEORY	Course Category	C	Professional Core	L	T	P	C
							3	1	0	4

Pre-requisite Courses	Nil	Co-requisite Courses	NIL	Progressive Courses	Nil
Course Offering Department	Mathematics	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	*To understand GCD and will be able to study about its classification of prime numbers*
CLR-2 :	*To relate the concepts of arithmetical functions*
CLR-3 :	*To understand concepts of averages arithmetic functions*
CLR-4 :	*To learn the concepts of some elementary theorems of prime numbers*
CLR-5 :	*To relate the concepts of Congruences*

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning			Program Learning Outcomes (PLO)														
		1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)	Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO - 3
CLO-1 :	*Students will be able to understand basic properties of prime number system*	1	85	80	L	L	L	H					M			L			
CLO-2 :	*Students become familiar with congruence relations and techniques of solving arithmetical functions*	3	80	75	L	L		M					M			L			
CLO-3 :	*Students will be able to understand the techniques of applying to solve number theoretic problems on averages arithmetic functions*	1	85	80	M	M		H					H			L			
CLO-4 :	*Students will be able to understand the concepts of some elementary theorems of prime numbers.*	3	80	75	L	M		H					M			L			
CLO-5 :	*Students become familiar with congruence relations and techniques of solving linear congruences*	1	85	80	M	M	L	M	L				M			L			

		Learning Unit / Module 1	Learning Unit / Module 2	Learning Unit / Module 3	Learning Unit / Module 4	Learning Unit / Module 5
Duration (hour)		12	12	12	12	12
S-1	SLO-1	*Introduction to fundamental theorem of arithmetic*	*Introduction to arithmetical functions*	*Introduction to averages arithmetic functions*	*Introduction to some elementary theorems of prime numbers*	*Introduction to Congruences*
	SLO-2	*The principle of induction*	*Mobius function*	*Definition of averages arithmetic functions*	*Chebyshev's functions*	*Definition and basic properties of Congruences*
S-2	SLO-1	*The well ordering principle*	*Euler totient function*	*The big oh notation*	*Relations*	*Example problems of Congruences*
	SLO-2	*Divisibility*	*Relation between Mobius function and Euler totient function*	***Asymptotic equality of functions***	*Relations connecting Chebyshev's functions*	*Equivalence relations of Congruences*

S-3	SLO-1	***Properties of Divisibility***	*A product formula for Euler totient function*	*Euler formula*	*Abel's identity*	*Fermat theorem*
	SLO-2	***Greatest Common Divisor***	*Properties of Euler totientfuntion*	*Euler summation formula*	*Prime number theorem*	*Fermat number*
S-4	SLO-1	*Tutorial 1: Discussion with case studies on fundamental theorem of arithmetic*	*Tutorial4 : arithmetical functions*	*Tutorial 7 : averages arithmetic functions*	*Tutorial 10: elementary theorems of prime numbers*	*Tutorial 13: Congruences*
	SLO-2	*Tutorial 1: Discussion with case studies on fundamental theorem of arithmetic*	*Tutorial4 : arithmetical functions*	*Tutorial 7 : averages arithmetic functions*	*Tutorial 10: elementary theorems of prime numbers*	*Tutorial 13: Congruences*
S-5	SLO-1	*Properties of GCD*	*The dirichlet product of arithmetical functions*	*Average order*	*Some equivalent forms of the Prime number theorem*	*Cancellation law*
	SLO-2	*Prime Numbers*	*Definition of arithmetical function*	*Some elementary asymptotic formula*	***Logically equivalent relations***	*Residue classes and complete residue system*
S-6	SLO-1	*Notations*	*Dirichlet and inverses and Mobius inversion formula*	*Average order of pi(n)*	*Asymptotic Logically equivalent relations*	*complete residue system modulo 'm'*
	SLO-2	*Prime number examples*	*Dirichlet multiplication*	*An application to the distribution of lattice points*	*Inequalities for pi(n) and nth prime*	*Linear congruences*
S-7	SLO-1	*Prime number theorem*	*Mobius inversion formula*	*Average order of d(n)*	*nth prime inequalities*	*Problems based on linear congruences*
	SLO-2	*The fundamental theorem of arithmetic*	*The Mangoldt function*	*Average order of divisor functions*	*Shapiro's Tauberian theorem*	*Reduced residue system*
S-8	SLO-1	*Tutorial 2: Prime numbers*	*Tutorial 5: Dirichlet and inverses and Mobius inversion*	*Tutorial 8: An application to the distribution of lattice*	*Tutorial 11: Tauberian theorem*	*Tutorial 14: Problems based on linear congruences*
	SLO-2	*Tutorial 2: Prime numbers*	*Tutorial 5: Dirichlet and inverses and Mobius inversion*	*Tutorial 8: An application to the distribution of lattice*	*Tutorial 11: Tauberian theorem*	*Tutorial 14: Problems based on linear congruences*
S-9	SLO-1	*The series of reciprocals of the primes*	*Multiplicative functions*	*An application to the distribution of lattice points visible from the origin*	*Applications of Shapiro's Tauberian theorem*	*Euler - Fermat theorem*
	SLO-2	*The Euclidean algorithm*	*Example problems of Multiplicative functions*	*The average of mu(n) and lambda(n)*	*Asymptotic formula for partial sums of prime*	*Little Fermat theorem*
S-10	SLO-1	*Division algorithm*	*Multiplicative functions and dirichlet multiplication*	*The partial sums of a Dirichlet product*	*partial sums of Mobius functions*	*Polynomial congruence modulo'p'*
	SLO-2	*GCD more than two numbers*	*Inverse of complete Multiplicative functions*	*Applications of mu(n) and lambda(n)*	*Elementary proof of the prime number theorem*	*Lagrange's theorem*
S-11	SLO-1	*GCD more than two numbers theorem*	*Liouville functions*	*Legendre identity*	*Brief sketch of an Elementary proof of the prime number theorem*	*The Chinese Remainder theorem*

	SLO-2	*GCD problems*	*The divisor functions*	*Another identity of partial sums*	*Selberg's asymptotic formula*	*Applications of The Chinese Remainder theorem*
S-12	SLO-1	*Tutorial 3: Division algorithm*	*Tutorial 6: Multiplicative functions*	*Tutorial 9: Dirichlet productApplications*	*Tutorial 12: Elementary proof of the prime number theorem and Selberg's asymptotic formula*	*Tutorial 15 : Applications of The Chinese Remainder theorem*
	SLO-2	*Tutorial 3: Division algorithm*	*Tutorial 6: Multiplicative functions*	*Tutorial 9: Dirichlet productApplications*	*Tutorial 12: Elementary proof of the prime number theorem and Selberg's asymptotic formula*	*Tutorial 15 : Applications of The Chinese Remainder theorem*

Learning Resources	1. David Burton, Elementary Number Theory, McGraw Hill Publication, 2017. 2. Joseph Silverman, A Friendly Introduction to Number Theory, 4th edition, Pearson Publication, 2019. 3. Tom M.Apostol, Introduction to Analytic Number Theory, Springer International Student Edition, Narosa Publishing House, New Delhi, 1976.	4. S.B. Malik, Basic Number Theory, 2nd Edition, S.Chand Publication, 2018. 5. H.S. Maan Sanjeev Kumar, Some Topics in Elementary Number Theory, INFOSTUDY Publication, 2018.

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*40 %*	-	30 %	-	20 %	-	25 %	-
Level 2	Apply Analyze	*40 %*	-	30 %	-	40 %	-	40 %	-
Level 3	Evaluate Create	*20 %*	-	40 %	-	40 %	-	35 %	-
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. **Mr.V.Maheshwaran, CTS, Chennai,** maheswaran@yahoo.com	*1.* **Dr. Y.V.S.S. Sanyasiraju, IIT Madras, Chennai,** sryedida@iitm.ac.in	***1. Dr. A. Govindarajan, SRMIST***
	2. Dr.K.C.SivaKumar, IIT Madras, Chennai, kcskumar@iitm.ac.in	***2. Dr. N. Parvathi, SRMIST***

Course Code	20ITC552J	Course Name	CRYPTOGRAPHY AND NETWORK SECURITY	Course Category	C	Professional Core	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLR-1 :	Understandthe OSI security architecture and classic encryption techniques			
CLR-2 :	Learnmathematics behind finite fields and number theory			
CLR-3 :	Understandthevarious block cipher and stream cipher models			
CLR-4 :	Understandthebasic concepts of networks, networking devices and various attacks possible on networking devices			
CLR-5 :	Understandthevarious methods and protocols to maintain E-mail security, and web security			

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning			Program Learning Outcomes (PLO)														
		1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)	Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research Skills	Team Work	Scientific Reasoning	Reflective Thinking	Self-Directed Learning	Multicultural Competence	Ethical Reasoning	Community Engagement	ICT Skills	Leadership Skills	Life Long Learning
CLO-1 :	Acquire fundamental knowledge on the concepts of finite fields and number theory	3	80	70	L	H	-	H	L	-	-	-	L	L	-	-	-	-	-
CLO-2 :	Acquire the ability to apply number theory concepts in Cryptography	3	85	75	M	H	M	M	H	-	-	-	M	L	-	-	-	-	-
CLO-3 :	Utilize the principles of public key cryptosystems, hash functions and digital signature	3	75	70	M	H	H	H	M	-	-	-	M	L	-	-	-	-	H
CLO-4 :	Acquire the ability to apply the concept of IP security and architecture	3	85	80	M	H	M	H	M	-	-	-	M	L	-	-	-	-	-
CLO-5 :	Apply the knowledge gained onthe various methods of password management and protocols to maintain system security	3	85	75	H	H	M	H	H	-	-	-	M	L	-	-	-	-	-

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Introduction, Finite Fields and Number Theory	IntroductiontoBlock Ciphers and Public Key Cryptography	Introduction to Hash Functions,Digital Signatures, Authentication functions	Introduction to Application Layer and Web Security	Introduction to Virtual Private Networks
	SLO-2	Security Services	Data Encryption Standard(DES) – Encryption process	Requirements of authentication functions	Networking Devices	VPN and its types
S-2	SLO-1	Security Mechanisms, Security attacks	DES Key generation process	Message authentication codes(MAC)functions	Layer1,2,3 devices	VPN architecture
	SLO-2	OSI security architecture, Network security model	DES decryption process	Requirements of Hash function	Firewall	Tunneling Protocols - I
S-3	SLO-1	Symmetric cipher model	DES example	MD5 algorithms	ACL	Tunneling Protocols - II
	SLO-2	Substitution techniques		SHA Algorithms	Packet Filtering	Tunnel mode
	SLO-1		Lab 4: DES implementation	Lab 7: SHA algorithm implementation	Lab 10: ACL configuration	Lab 13:IPS configuration

S 4-5	SLO-2	*Lab 1: Substitution techniques*				
S-6	SLO-1	*Transposition techniques*	*Block cipher modes of operation*	*Digital signatures*	*DMZ*	*IPSEC - Introduction*
	SLO-2	*steganography*	*AES*	*Digital signatures requirements*	*Alerts,Audit Trials*	*IPSEC architecture,*
S-7	SLO-1	*Groups, Rings, Fields*	*Blowfish*	*Digital signature Standard*	*IDS , IPS*	*Components*
	SLO-2	*Modular arithmetic*	*RC5 algorithm- encryption process*	*Requirements of DSS*	*IDPS and types*	*Examples*
S-8	SLO-1	*Euclid's algorithm*	*Principles of public key cryptosystems*	*ElgamalDigital signature Scheme*	*SSL/TLS Basic Protocol*	***IPSEC Protocol suite***
	SLO-2	*Finite fields*	*RSA algorithm, example*	*Example.*	*Computing the keys, Client authentication*	*Architecture, functionalities*
S9-10	SLO-1	*Lab 2:Implement Euclid and extended Euclid Algorithm*	*Lab 5:Implement RSA Algorithm*	*Lab 8: Implement Elgamal DSS*	***Lab 10: Extended ACL configuration***	*Lab 14:IPSec VPN Authentication*
	SLO-2					
S-11	SLO-1	*Polynomial Arithmetic*	*Key management process*	*SchnorrDigital signature Scheme*	*PKI as deployed by SSL*	*Transport Mode, Authentication Header*
	SLO-2	*Prime numbers,Testing for primality*	*Key management requirements*	*Schnorr DSS example*	*Attacks fixed in v3*	***Introduction to*** *Encapsulation Security Payload (ESP)*
S-12	SLO-1	*Fermat's theorem*	*DiffieHellman Key exchange algorithm*	*Applications*	*Exportability, Encoding*	*IKE Phase I, II*
	SLO-2	*Euler's theorem*	*Diffie Hellman Key exchange algorithm - Examples*	*Authentication protocols*	*Secure Electronic Transaction (SET)*	*Generic Routing Encapsulation (GRE).*
S-13	SLO-1	*The Chinese Remainder theorem*	*Introduction to ECC (Elliptic Curve Cryptography)*	*Authentication protocols - requirements*	*Kerberos*	*AAA authentication requirements*
	SLO-2	*Discrete logarithms.*	*Elliptic curve arithmetic*	*Case study*	*Applications*	*Applications*
S14-15	SLO-1	*Lab 3:Implement Chinese Remainder Theorem*	*Lab 6: Implement Diffie Hellman Algorithm*	*Lab 9: Implement Schnorr DSS*	*Lab 12: Understanding Kerberos*	*Lab15:Configuring AAA Authentication*
	SLO-2					

Learning Resources	3. *William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson Education, 2003.* 4. *Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security", Prentice Hall,2 nd edition, ISBN-10: 0130460192, ISBN-13: 978-0130460196, 2002.*	5. *Charles Pfleeger," Security in Computing", Prentice Hall, 4 th Edition, ISBN-10: 0132390779, ISBN-13: 978-01323907744, 2006. Earl Gose, Richard Johnsonbaugh, Steve Jost, "Pattern Recognition and Image Analysis", Prentice Hall of India Private Ltd., New Delhi – 110 001, 1999.*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
	Understand								
Level 2	Apply	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
	Analyze								
Level 3	Evaluate	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Create								
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. *Ms.SaliniKotari, Associate consultant, KPMG, Chennai.*		1. *Ms.C.Fancy, SRMIST, KTR*
2. *Mr.VishwaPrasath.T.S., Security Analyst, Crossbow Labs, Bangalore.*		2. *Ms.G.Sujatha, SRMIST KTR*

Course Code	20ITC553J	Course Name	MALWARE ANALYSIS	Course Category	C	Professional Core Course	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	INFORMATION TECHNOLOGY	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:	Learning			Program Learning Outcomes (PLO)														
		1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)	Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
CLR-1 :	Understand the fundamentals of static and dynamic analysis.																		
CLR-2 :	Gain knowledge about running malware in virtual environment.																		
CLR-3 :	Study about disassembly constructs and its structures.																		
CLR-4 :	Study about new processors and file types using the IDA SDK																		
CLR-5 :	Explore popular plug-ins that make writing IDA scripts easier, allow collaborative reverse engineering																		
CLR-6	Understand how to best approach the subject of Android malware threats and analysis.																		
Course Learning Outcomes (CLO):	*At the end of this course, learners will be able to:*																		
CLO-1 :	Gain knowledge about the different forms of malware.	1	80	70	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M
CLO-2 :	Set up a safe virtual environment to analyze malware.	1	85	75	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M
CLO-3 :	Navigate, comment, and modify disassembly.	1	75	70	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M
CLO-4 :	Use code graphing to quickly make sense of cross references and function calls	2	85	80	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M
CLO-5 :	Use IDA's built-in debugger to tackle hostile and obfuscated code.	2	85	75	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M
CLR-6	Learn procedures for recognizing and analyzing malware quickly and effectively using OllyDbg.	2	80	70	H	H	H	H	M	L	M	H	M	H	M	H	H	H	M

Duration (hour)		15	15	15	15	15
S-1	SLO-1	*INTRODUCTION: What Is Malware?Why Malware Analysis?*	*DYNAMIC ANALYSIS :System And Network Monitoring*	*IDA:x64 Architecture-Analyzing 32-bit Executable On 64-bitWindows*	*Malware Functionalities andPersistence-:Functionalities*	*OLLYDBG: Loading Malware*
S-2	SLO-2	*Types Of Malware Analysis*	*Dynamic Analysis (Monitoring) Tools- Process Inspection with Process Hacker*	*Disassembly Using IDA-Code Analysis Tools*	Malware Persistence Methods	*The OllyDbg Interface*
S-3	SLO-1	*Malware Sources*	*Determining System Interaction with ProcessMonitor*	*Static Code Analysis (Disassembly) UsingIDA*	*Virtual Memory and its use in Operating System.*	*Memory Map and its management.*
S 4-5	SLO-1				*LAB 10- PERFORM VALIDATION*	

	SLO-2	*LAB 1 : SETTING UP THE LAB ENVIRONMENT*	*LAB4: DYNAMIC MALWARE ANALYSI-ZERO ACCESS TROJAN*	*LAB7- HELLO WORLD PROGRAM USING NASM IN LINUX*	*USING GDB DEBUGGER FOR BINARY FILES.*	*LAB 13-DEBUGGING A VULNERABLE C++ APPLICATION*
S-6	SLO-2	*Static Analysis- Determining the File Type*	*Logging System Activities Using Noriben*	*Exploring IDA Displays*	*User Mode And Kernel Mode*	*First and Second chance Exception, Common exceptions in Malware Payload.*
S-7	SLO-1	*Identifying File Type Using Manual Method, Python and Tool Method*	*Capturing Network Traffic With Wire shark*	*Improving Disassembly Using IDA*	*Code Injection Techniques,* Hooking Techniques	*Patching options in OllyDbg, Standard Plug-in with DLL's.*
S 9-10	SLO-1 SLO-2	*LAB2: CREATE SIMPLE VIRUS USING NOTEPAD, VBSCRIPT AND ANALYZE IN SANDBOXING ENVIORNMENT.*	*LAB5: SHELL CODE ANALYSIS – NETCAT COMMAND*	*LAB8- PERFORMING STATIC ANALYSIS OF MALWARE PAYLOAD USING IDA PRO*	*LAB 11- EXTRACTING STRINGS, INSPECTING PE HEADER OF PAYLOAD*	*LAB14- ANALYZING ENCRYPTED MALWARE USING TOOL*
S-11	SLO-2	*Determining Cryptographic Hash in Python*	*Dynamic-Link Library (DLL) Analysis*	*IDA Python*	*Custom Encoding/Encryption*	*Viewing Threads and Stacks*
S-12	SLO-1	*Multiple Anti-Virus Scanning*	Computer Basics- Memory-How Data Resides In Memory-*CPU*	*Debugging Malicious Binaries*	*Malware Unpacking*	Executing Code and its impact
S-13	SLO-2	*Scanning the Suspect Binary with Virus Total*	Program Basics- CPU Registers	*Debugging a Binary Using x64dbg*	*Displaying Device Trees*	*Purpose of Breakpoints*
S 14-15	SLO-1 SLO-2	*LAB3: DYNAMIC MALWARE ANALYSIS- LOTTERY.TXT*	*LAB 6:IMPLEMENTING COVERT CHANNEL- REMOTE ACCESS TROJAN*	*LAB9: STATIC ANALYSIS OF MALWARE PAYLOAD WITH OllyDbg*	*LAB12- GENERATING CRYPTOGRAPHIC HASH USING TOOLS*	*LAB 15- PATCHING BINARY USING IDA* *IDA SCRIPTING AND PLUGINS*

Learning Resources	1. *Monnappa K A,Learning Malware Analysis, Published by Packt Publishing Ltd, 1st Edition 2018.* 2. *Michael Sikorski,Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press; 1 edition (February 1, 2012).*	3. *Chris Eagle, the IDA Pro Book, 2nd Edition, No Starch Press, 2011.* 4. *Ken Dunham, Android Malware and Analysis, Kindle Edition, Auerbach Publications.*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. Mr. K.Santhosh, *Information Security Risk Analyst,* *PricewaterhouseCoopers Pvt Ltd, Bangalore, Karnataka 560008.* *Email: santhoshshivam72@gmail.com*	*1. Dr.L.Kavisankar* *Associate Professor,* *Dept. Of CSE, Hindustan Institute of Science and Technology* *Email: lkavis@hindustanuniv.ac.in*	*1. Mr. V. Joseph Raymond, SRMIST, KTR*

Course Code	20ITC554J	Course Name	Forensic and Incident Response	Course Category	C	Professional Core Course	L	T	P	C
							3	0	2	4

Pre-requisite Courses		Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the basic of forensic investigation and its procedure, policies on laws
CLR-2 :	Understand the network, filesystem , user system level forensic
CLR-3 :	Acquire knowledge in investigation procedure and its policies
CLR-4 :	Exploring new aspect in investigation in every
CLR-5 :	Understand the role of incident response team
CLR-6 :	Implement and analyze the evidence to formulate the strategy

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning			Program Learning Outcomes (PLO)														
		1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)	Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
CLO-1 :	Apply the knowledge forensic investigation	2	80	70	H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-2 :	Identify and design the attack scenario for volatile & non volatile	3	85	75	H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
CLO-3 :	Implement and investigate the procedure evolve in forensic duplication	3	75	70	H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
CLO-4 :	Identify , implement and investigate on the hard disk imaging	1	85	80	H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-5 :	Identify and investigate the network and browser forensic	1	85	75	H	-	-	H	-	-	-	-	-	-	-	-	-	-	-
CLO-6 :	Design and implement the file system , forensic report writing	3	80	70	H	H	H	H	H	-	-	-	-	-	-	-	M	-	M

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Introduction to incident response process-	Introduction to evidence data collection -Volatile	Introduction to evidence data collection – Non volatile	Introduction to analyses / Detect malicious code and intruders	Introduction to file system analysis
	SLO-2	Incident response methodology	Volatile data collection - Windows	Introduction to computer storage fundamentals Hard drives and interfaces	System process, Unusual or hidden files	How Files Are Compiled
S-2	SLO-1	Incident process	Creating Response tool kit	Preparation of hard drive media	Root kits and backdoors	Statically Linked Programs
	SLO-2	Preparation for incident response – Overview	Storing Information Obtained during the Initial Response	Introduction to files system and storage layers	Introduction to network forensic	Dynamically Linked Programs
S-3	SLO-1	Preincident preparation	Obtaining Volatile Data	Introduction to files system and storage layers	Introduction to browser forensic	Compilation Techniques and File Analysis

	SLO-2	*Preparing Individual Hosts*	*Performing an In-Depth Live Response*	*Forensic duplication*	*Types of network monitoring*	*Static Analysis of a Hacker Tool*
S 4-5	SLO-1 SLO-2	*Lab 1: lab setup for pre-incident preparation*	*Lab 4: Memory / Process data collection –Volatility*	*Lab 7: Hard drive imaging / Logical*	*Lab 10: How to collect network logs for investigation Firewall logs, Virus logs*	*Lab 13: Browser Forensic*
S-6	SLO-1	*Preparing a Network*	*Volatile data collection – Unix*	*Qualified forensic duplicate*	*Browser Investigation*	*NTFS_File system category, content category*
	SLO-2	*Establishing Appropriate Policies and Procedures*	*Storing Information Obtained During the Initial Response*	*Overview of evidence handling procedures- Chain of custody*	*Browser Investigation Firefox- IE*	*NTFS_Metadata category, Filename category*
S-7	SLO-1	*Creating a Response Toolkit .*	*Obtaining Volatile Data Prior to Forensic Duplication*	*Forensic Duplicates As Admissible Evidence*	*Browser Investigation -Firefox*	*NTFS_Application - Specific file system*
	SLO-2	*Establishing an Incident Response Team*	*Introduction to Memory*	*Forensic Duplication Tool Requirements*	*Case Study : Browser Investigation*	*NTFS_Application level search technique*
S-8	SLO-1	*Overview of the Initial Response Phase*	*Process data collection*	*Creating a Forensic Duplicate of a Hard Drive*	*Case study : Report Writing*	*Comparison of windows (FAT/ EXFAT/NTFS*
	SLO-2	*Establishing an Incident Notification Procedure*	*Introduction to windows process*	*Creating a Qualified Forensic Duplicate of a Hard Drive*	*Network Investigation*	*EXT_File system category, content category*
S 9-10	SLO-1 SLO-2	*Lab 2- Volatile data collection – Windows / Linux / Critical system log*	*Lab 5: Registry*	*Lab 8: Malware Forensics*	*Lab 11 : Network Forensic using TCP Dump/ Wireshark*	*Lab 14: NTFS File system*
S-11	SLO-1	*Recording the Details after Initial Detection*	*Recycle bin and data storage*	*Creating a Qualified Forensic Duplicate with SafeBack*	*Finding Network-Based Evidence*	*EXT_Metadata category, Filename catagory*
	SLO-2	*Incident Declaration*	*Introduction to registry structure*	*Evidence system description, Evidence tags*	*Generating Session Data with tcptrace*	*EXT_Application level search technique*
S-12	SLO-1	*Investigation Guidelines*	*Evidence collection from registry – System, Application*	*Evidence label, storage , backup , disposition*	*Checking for SYN Packets*	*Comparison of Linux (EXT 2/3/4/ MacOS)*
	SLO-2	*Legalities of Forensic-*	*Evidence collection from registry*	*Case Study : Evidence Handling reporting*	*Reassembling Sessions Using tcpflow*	*Case Study : File system*
S-13	SLO-1	*Reason for Legal , Statutory*	*Evidence collection from network*	*Case study : Report Writing*	*Reassembling Sessions Using Ethereal*	*Forensic Report Writing*
	SLO-2	*Governmental laws: US*	*Analysis on evidence collection*	*Evidence Custodian audits*	*Refining tcpdumpFilters .*	*Case study Report Writing*
S 14-15	SLO-1 SLO-2	*Lab 3- Volatile data collection – Windows / Linux*	*Lab 6: Hard drive imaging / Physical using tool/ Linux commands*	*Lab 9 : Investigation on static malicious code*	*Lab 12 : Disk Forensics*	*Lab 15:EXT file system*

Learning Resources	1. *Kevin Mandia, Chris Prosise, "Incident Response and computer forensics", Tata McGrawHill,2006.* 2. *Peter Stephenson, "Investigating Computer Crime: A Handbook for Corporate Investigations", Sept 1999* 3. *Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, 1st Edition, 2001* 4. *Skoudis. E., Perlman. R. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall Professional Technical Reference. 2001* 5. *Norbert Zaenglein, "Disk Detective: Secret You Must Know to Recover Information from a Computer", Paladin Press, 2000*	6. *Kevin Mandia , "Incident Response & Computer Forensics, 3rd Edition" : 2012. The McGraw:Hill, ISBN-13: 978-0071798686* 7. *Douglas Schweitzer ,"Incident Response - Computer Forensics Toolkit", Copyright © 2003 by Wiley Publishing, Inc, ISBN: 0-7645-2636-7* 8. *AymanShaaban ,Konstantin Sapronov "Practical Windows Forensics - Leverage the power of digital forensics for Windows systems" , Packt Publishing, June 2016 , ISBN 978-1-78355-409-6* 9. *Leighton R. Johnson III ,"Computer Incident Response and Forensics Team Management",Syngress ISBN: 978-1-59749-996-5* 10. *Brian Carrier "File System Forensic Analysis" – by Addison Wesley, 1st edition,2005. ISBN-13: 978-0321268174*

Learning Assessment

	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 #(15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers

Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
	*1.*Mr.*Ashok Kumar Mohan , Amrita University* 2. Ms. Chita , SSN college of Engineering	*1. Ms. Kirthiga Devi T, SRMIST, KTR*

ACADEMIC CURRICULA

Professional Elective Courses

M.TECH

INFORMATION SECURITY AND CYBER FORENSICS

Academic Year – 2020-2021

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

Kattankulathur, Chengalpattu District, Tamil Nadu, India

Course Code	20ITE555J	Course Name	ANDROID SECURITY AND DESIGN INTERNALS	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the fundamentals of Android Stack.
CLR-2 :	Gain knowledge about running Android App in Sandboxing environment.
CLR-3 :	Analyzing Android traffic and forensics.
CLR-4 :	Using SQLite understanding storing and retrieving of data.
CLR-5 :	Learn ARM Architecture and its features.

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Learn about the security model in Android architecture.	1	80	70
CLO-2 :	Implement the process of running App and debug its features.	1	85	75
CLO-3 :	Gain knowledge about the various types of Android Forensics.	1	75	70
CLO-4 :	Understanding the handling of database.	2	85	80
CLO-5 :	Learn about exploring Android malwares.	2	85	75

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
L	H	-	H	L	-	-	-	L	L	-	-	-	-	-
M	H	M	M	H	-	-	-	M	L	-	-	-	-	-
M	H	H	H	M	-	-	-	M	L	-	-	-	-	H
M	H	M	H	M	-	-	-	M	L	-	-	-	-	-
H	H	M	H	H	-	-	-	M	L	-	-	-	-	-

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Android security model:linux kernel	Basics:creating an android virtual device	Analysis: android traffic interception	Exploit: understanding sqlite in depth	Security features: app data and backup
S-2	SLO-2	Native user space	Android debug bridge for connecting devices	Ways of android traffic analysis.	Analyzing an simple application	Activities and implement with security parameters
S-3	SLO-1	Understanding dalvik vm and its purpose.	Burp suite for analyzing traffic.	Https proxy interception	Security vulnerability and its impact.	Notifications used in android app and secured approach.
S 4-5	SLO-1	Lab 1 : setting up the lab environment	Lab 4: dex analysis of apk file	Lab 7: analyzing android malware	Lab10: drozer scripting and exploring vulnerability	Lab 13-debuging with andbug and jdb
	SLO-2					
S-6	SLO-2	Applications- sandboxing	Auditing android applications	Extracting sensitive files from packet capture	Android web view vulnerability-using web view	Security services and its impact.
S-7	SLO-1	Code signing and platform key	Content provider leakage	Android forensics- types of forensics	Identifying vulnerability	Security with http and ssl
S-8	SLO-2	Selinux in android stack	Insecure file storage	File systems in android stack and	Infecting legitimate apk's.	Custom account type

				its impact		
S9-10	SLO-1 SLO-2	*Lab2 : understanding android permissions and apk signing*	*Lab 5: android debug bridge and log based vulnerabilities*	*Lab8- traffic analysis and ssl pinning*	Lab 11- understanding dropbox vulnerability	Lab 14- automated hooking with introspy and cydia substrate
S-11	SLO-1	*Android startup process*	*Owasp top 10 for mobile*	*Using af logical*	*Arm architecture- execution modes*	*Security tips for developing app*
S-12	SLO-2	*System services of android stack*	*Android application teardown*	*Dumping applications*	*Simple stack based buffer overflow.*	*Custom rom*
S-13	SLO-1	*Ipc- binder's- framework libraries*	*Exploring the apk tool*	*Logging the logcat*	*Return oriented programming.*	*Managing web view objects*
S 14-15	SLO-1 SLO-2	*Lab3: android application components*	*Lab6: reversing android applications*	*Lab 9: leaking content provider,read based content provider vulnerability*	*Lab12- exploting malicious payload with metasploit*	*Lab15- hooking using xposed and androguard*

Learning Resources	1. *Gupta Aditya, Learning Pen testing for Android Devices, Packt Publishing, 2014.* 2. *NikolayElenkov, Android Security Internals: An In-Depth Guide to Android's Security, reprint, No Starch Press, 2014.*	3. *Jeff Six, Application Security for the Android Platform, O'Reilly Media, Inc., 2011.* 4. *Internet Resource-https://developer.android.com/guide*

Learning Assessment

	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers

Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. *Mr. K.Santhosh,Information Security Risk Analyst,PricewaterhouseCoopers Pvt Ltd, Bangalore, Karnataka 560008.Email: santhoshshivam72@gmail.com*	1. *Dr.L.KavisankarAssociate Professor,Dept. Of CSE, Hindustan Institute of Science and Technology, lkavis@hindustanuniv.ac.in*	1. *Mr. V. Joseph Raymond, ,SRMIST, KTR*

Course Code	20ITE556J	Course Name	CLOUD ARCHITECTURES AND SECURITY	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the fundamentals of cloud computing
CLR-2 :	Understand the requirements for an application to be deployed in a cloud.
CLR-3 :	Exploring the services and techniques in cloud security concepts
CLR-4 :	Implement and analyze the various cloud protection mechanisms
CLR-5 :	Become knowledgeable in the methods and standards to secure cloud.

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking	Expected Proficiency	Expected Attainment
CLO-1 :	Apply the knowledge of cloud computing services	2	80	70
CLO-2 :	Identify and design the cloud application development scenarios	3	85	75
CLO-3 :	Design and implement the security principles to cloud computing	3	75	70
CLO-4 :	Identify and implement cloud security with respect to cloud computing attack surfaces	1	85	80
CLO-5 :	Apply the knowledge gained on Cloud computing standards and security management	1	85	75

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering	Problem Analysis	Design & Development	Analysis, Design,	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	-	H	-	-	-	-	-	-	-	-	-	-	-

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Cloud Computing Fundamentals	Cloud Applications	Information and NetworkSecurity Concepts	Multi-tenancy software	Security management in the cloud, Data security and storage in cloud
	SLO-2	Cloud Computing definition, private, public and hybrid cloud	Software as a service and cloud computing	Confidentiality and Data Protection, Availability	Multi-tenancy Issues	StorageSecurity- HIDPS
S-2	SLO-1	Cloud types; IaaS, PaaS, SaaS	Successful SaaS architectures	Authentication, non-repudiation, availability, access control	Isolation of users/VMs from each other	log management and analysis
	SLO-2	Benefits and challenges of cloud computing	Dev 2.0 platforms	Identity and Access management	How the cloud provider can provide this	Data Loss Prevention and recovery
S-3	SLO-1	Migrating to the Cloud - Technical considerations	Dev 2.0 in the cloud for enterprises	defense in depth approach	multi-tenant cloud software architecture	Responsibility, ownership of data,
	SLO-2	Main players in the Field, Overview of Security Issues	advantages and disadvantages	least privilege techniques	Architectural concerns in multi-tenant cloud applications	right to penetration test
S 4-5	SLO-1		Lab 4: Demo on Dev 2.0 platforms			

Duration (hour)		15	15	15	15	15
	SLO-2	*Lab 1: Demo on Cloud computing services*		***Lab 7:** Specific Linux commands and Buffer Overflow vulnerability*	***Lab 10: Demo on** Multi-tenancy configurations / software*	***Lab 13:** Demo on Cloud Storage Security*
S-6	SLO-1	*Public vs Private clouds*	*Technologies and the processes required when deploying web services*	*how computer security concepts apply in the cloud and their importance in PaaS, IaaS and SaaS*	*Virtual machine technology*	*Security management standards*
	SLO-2	*role of virtualization in enabling the cloud*	*Deploying a web service from inside and outside a cloud architecture*	*Cryptographic Key Management Issuesand Challenges in Cloud Services*	*Virtualization System Vulnerabilities*	*SaaS, PaaS, IaaS availability management*
S-7	SLO-1	*Technologies for virtualization in cloud computing*	*Web services: SOAP and REST*	*Challenges in Cryptographic Operations*	*Virtualization System Security Issues*	
	SLO-2	*Load Balancing and Virtualization*	*SOAP API versus REST API*	*Key Management for IaaS*	*ESX and ESXi Security*	*The International Organization for Standardization (ISO) - 27017, 27018, 27001*
S-8	SLO-1	*Understanding Hypervisor*	*AJAX: asynchronous 'rich' interfaces*	*Challenges in Cryptographic Operations*	*ESX file system security*	*NIST standards to cloud computing security*
	SLO-2	*Private Cloud Providers Compare - Microsoft, VMware, OpenStack*	*Mashups: user interface services*	*Key Management for Pass and Saas*	*storage considerations*	*Cloud Security Alliance recommendations*
S9-10	SLO-1	*Lab 2: Demo on cloud Deployment models*	*Lab 5: Demo o SOAP and REST with a case study*	*Lab 8: OpenSSL commands for cryptography operations*	*Lab 11: Demo on VMware ESXi security configurations*	*Lab 14: Demo on ISO, NIST standards*
	SLO-2					
S-11	SLO-1	*Business Agility*	*Development environments for service development*	*Cloud Architectural Considerations - General Issues*	*Data in the cloud*	*Legal and Compliance issues in cloud computing*
	SLO-2	*The SPI Framework, How Those Applications Help Your Business*	*Amazon, Azure, Google App.*	*User authentication in the cloud*	*Cloud file systems: GFS and HDFS*	*Examination of modern Security Standards (eg PCIDSS)*
S-12	SLO-1	*Benefits to Cloud architecture*	*custom enterprise application and Dev 2.0*	*Identity Management and Access Control*	*BigTable, HBase and Dynamo*	*how standards deal with cloud services and virtualization*
	SLO-2	*Challenges to Cloud architecture*	*Modeling and Design of a Cloud Workflow*	*Working With Policies - Identity Based IAM Policies*	*Cloud data stores: Datastore and SimpleDB*	*Regulatory mandates and audit policies*
S-13	SLO-1	*NIST Cloud Computing Reference Architecture*	*Implementing workflow in an application*	*Using Policies To Access Resources*	*Cloud Storage Services for Multi-Cloud*	*compliance requirements for Cloud based infrastructures*
	SLO-2	*Architectural Design Challenges*	*Workflow as a Service in the Cloud*	*Secure Execution Environments and Communications*	*Backup and Disaster recovery*	*compliance for the cloud provider vs. compliance for the customer*
S14-15	SLO-1	*Lab 3: Demo on Business use cases adopting cloud computing*	*Lab 6: Demo on Workflow in the cloud application*	*Lab 9: Demo on Identity Management and Access Control*	*Lab 12: Demo on Cloud data stores*	*Lab 15: Demo on modern security standards*
	SLO-2					

Learning Resources	1. *GautamShroff, Enterprise Cloud Computing Technology Architecture Applications [ISBN: 978-0521137355]* 2. *Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach [ISBN: 0071626948]* 3. *Ronald L. Krutz, Russell Dean Vines, Cloud Security - A Comprehensive Guide to Secure, Wiley Publishing,ISBN: 978-0-470-58987-8* 4. *Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, ISBN: 978-0-596-80276-9*

Learning Assessment

	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
		1. *Mr. Savaridasan, SRMIST, KTR*

Course Code	20ITE557J	Course Name	SECURITY SCRIPTING AND ANALYSIS	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	To gain mastery over scripting
CLR-2 :	To gain mastery over application to problems in computer and network security
CLR-3 :	Practice packet analysis automation using their own scripts
CLR-4 :	Understand the secure code development
CLR-5 :	Understand and practice exploit analysis techniques
CLR-6 :	Understand and expertise over the tool wireshark

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Learn the system and network security programming	2	80	70
CLO-2 :	Acquire knowledge on developing web servers and clients	3	85	75
CLO-3 :	Develop their own packet capturing and analyzing tools	3	75	70
CLO-4 :	Develop source code vulnerability detecting scripts	1	85	80
CLO-5 :	Learn exploit analysis tools	1	85	75
CLO-6 :	Learn network security analysis using packet capturing tools	3	80	70

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design,	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	-	H	-	-	-	-	-	-	-	-	-	-	-
H	H	H	H	H	-	-	-	-	-	-	-	M	-	M

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Introduction to InterpretedLanguage	Raw Socket programming	Web Servers	Exploit Development techniques-introduction	Wireshark- introduction
	SLO-2	Coding standards and data types	Packet injection using raw socket programming	Client side scripting	Types of exploit development techniques	Capturing methodologies
S-2	SLO-1	Mutable and immutable datatypes comparison in memory level	Socket Libraries and its functionalities	HTML basics	Immunity Debuggers and Libs	Capture filters
	SLO-2	Variables, operators and Expressions	Programming server clients using TCP	CGI scripts	Attaching and detaching process	Display filters
S-3	SLO-1	Program Structure and Control statements	Asynchronous socket channels	Web Application Fuzzers	Writing plugins for Immunity debugger	Searching for packets using the Find dialog

Duration (hour)		15	15	15	15	15
	SLO-2	Loops - different types of for, while	Programming Servers and Clients using UDP	Types of fuzzing techniques	Malware sample analysis	Create new Wireshark profiles
S4-5	SLO-1	Lab 1: Logical programs using list,tuple,loops,control statement	Lab 4: Syn flood using raw socket	Lab 7: Server and client side scripting	Lab 10: Immunity debugger malware tool exploration	Lab 13: New profile creation in wireshark
	SLO-2					
S-6	SLO-1	Functions and lambda expression	Multithreaded server-TCP and UDP	Scraping Web Applications-introduction	Advanced exploitation techniques	Usage of Graphs
	SLO-2	Examples for different types functions	Example programs applying multithreaded server concepts	Remote file access -Urlopen, urlretrive	Writing payloads for exploitation	IO,TCP,Flow Graphs
S-7	SLO-1	Classes, Objects and Other OOPS Concepts	Scapy Introduction	Beautiful soup-urllib	Buffer overflow attack	Inspection of Application Layer protocols
	SLO-2	Scope of variables-class level, instance level and local	Packet crafting using scapy	HTML parsing	Example with immunity debugger	DNS,FTP, HTTP, SMTP
S-8	SLO-1	Inheritance and Overloading-types and examples	Programming Wired Sniffers-scapy	XML file analysis	Pyhook introduction	Colourcoding
	SLO-2	Exception handling	Packet injection –scapy wired	Examples for XML file analysis	Examples for pyhook key loggers	Creation of colouringrules
S9-10	SLO-1	Lab2: Application using exception, inheritance and operator overloading	Lab 5: Wired sniffing using scapy	Lab 8: Web scrapping	Lab 11: **Exploit analysis**	Lab 14: InspectingApplication Layer protocols
	SLO-2					
S-11	SLO-1	Introduction to IO streams and programming in file concepts	Programming Wireless Sniffers-scapy	Web Browser Emulation-introduction	Source code vulnerability - introduction	Analyzing Transport Layer Protocol
	SLO-2	Directory Access and file traversing	Wireless sniffers examples	Mechanize- examples	Source code vulnerability analysis	TCP-UDP
S-12	SLO-1	Creation of Threads and its need	Programming arbitrary packet Injectors- wireless	Application Proxy	Static source code vulnerability detection -scripting	Analyzing packets for security tasks
	SLO-2	Multithreading and Concurrency using locks and synchronization	Packet injection examples	Own proxy creation	Example scripts for static detection	Security analysis methodology
S-13	SLO-1	Inter Process Communication (IPC)	Read and write to pcap file -scapy	Attacking Web Services	dynamic source code vulnerability detection-scripting	Scans and sweeps
	SLO-2	Permissions and Controls	Attack automation using scapy	Examples for attacking web services	Example methods for dynamic detection	ARP ICMP TCP UDP
S14-15	SLO-1	Lab 3: Application applying IPC and thread concepts	Lab 6: Wireless sniffing	Lab 9: Browser emulation	Lab 12: Finding source code vulnerability	Lab 15: Network Security Analysis using wireshark
	SLO-2					

Learning Resources	1. *Mike Dawson,"More Python programming for Absolute Beginner", CengageLearning PTR;· 3rd edition, ISBN-10: 1435455002, ISBN-13: 978-14354550092, 2010.* 2. *The Web Application Hacker's Handbook, 2nd Edition, Wiley Publication, DafyddStuttard, Marcus Pinto* 3. *Mastering Wireshark, PACKT Publishing, By Charit Mishra, March 2016* 4. *Mark Lutz," Python Pocket reference", O'Reilly Media; 4 th edition, ISBN-10: 0596158084, ISBN-13: 978-0596158088, 2009.* 5. *Wireshark essentials by James H.Baxter, 2014*

Learning Assessment

	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers

Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
		1. *Mrs. Monica Catherine* *Assistant Professor,* *Department of IT,SRMIST, KTR*

Course Code	20ITE558J	Course Name	PRINCIPLES OF SECURE CODING	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the need for secure coding
CLR-2 :	Understand the importance of proactive development process
CLR-3 :	Explain and demonstrate secure coding practices
CLR-4 :	Learn input issues related to database and web applications
CLR-5 :	Exploring the principles of software security engineering

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Apply the knowledge of secure coding	2	80	70
CLO-2 :	Identify and design the systems with defensive capabilities	3	85	75
CLO-3 :	Identify and correct the vulnerable code in development	3	75	70
CLO-4 :	Identify the database and web application vulnerability and to protect with secure practices	1	85	80
CLO-5 :	Apply securesoftware engineering practices	1	85	75

		Program Learning Outcomes (PLO)														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design,	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
CLO-1 :	Apply the knowledge of secure coding	H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-2 :	Identify and design the systems with defensive capabilities	H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
CLO-3 :	Identify and correct the vulnerable code in development	H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
CLO-4 :	Identify the database and web application vulnerability and to protect with secure practices	H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
CLO-5 :	Apply securesoftware engineering practices	H	-	-	H	-	-	-	-	-	-	-	-	-	-	-

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Introduction to secure coding principles.Need for secure systems.	Secure coding in C - Character strings	Integer security - Integer Data Types	Database and web specific input issues	Software security engineering – Software Assurance, Faults and Vulnerabilities
	SLO-2	ideas for instilling Security culture and deploying Information Security culture frameworks	Common String manipulation errors	Integer Conversions	SQL injection - Quoting the Input	Vulnerability Reporting, Vulnerability Classifications
S-2	SLO-1	Attackers advantage and defenders dilemma	String Vulnerabilities	Integer Operations and	Use of stored procedures and its security	Threats to software, Secure Systems Engineering
	SLO-2	Proactive security	String vulnerabilities exploitation	Integer Vulnerabilities at runtime	Insecure direct object references	Software requirements engineering
S-3	SLO-1	Design phase considerations	Mitigation strategies for strings	verification of integer based vulnerabilities at testing phase	Database Security applying Statistical Method.	Methods, Techniques and tools for secure software

Duration (hour)		15	15	15	15	15
	SLO-2	*Development and test phase considerations*	*Obsolete functions and secure functions by standards*	*Mitigation strategies for Integer based vulnerabilities*	*Database Security Solutions*	*Software Assurance Maturity Model, Secure Software Development Life Cycle Processes*
S4-5	SLO-1	*Lab 1: study on proactive security principles*	*Lab 4:Demo on string vulnerabilities and mitigation*	*Lab 7:Demo on integer security*	*Lab 10: Demo on SQL injection*	*Lab 13: Demo on software threats and tools for secure software*
	SLO-2					
S-6	SLO-1	*Security principles to live by – SD3*	*C Dynamic Memory Management*	*Formatted OutputFunctions*	*Browser Security principles*	*Misuse and abuse cases , SQUARE process model*
	SLO-2	*Security principles*	*Common errors in memory management*	*Stack Randomization, Format String Vulnerabilities*	*Exceptions to same-origin policy*	*Security Design patterns*
S-7	SLO-1	*Secure design through threat modeling*	*Instruction pointer modification*	*Exploiting Formatted Output Functions*	*Cross site scripting related attacks and remedies*	*Software security practices*
	SLO-2	*Security Techniques*	*Targets for instruction pointer modification*	*Buffer Overflow, Code injection*	*Cross site request forgery*	*Software security analysis and testing*
S-8	SLO-1	*Threat Modeling Tools*	*Referencing Freed Memory*	*Stack Randomization*	*Broken Authentication*	*Approach, Types, and Tools*
	SLO-2	*Security Into DevOps Processes*	*Mitigation strategies in pointer basedvulnerabilities*	*Mitigation Strategies for formatted function vulnerabilities*	*Mitigating web server attacks*	*Dynamic Application Security Testing Tools*
S9-10	SLO-1	*Lab 2: Demo on Threat model*	*Lab 5: Demo on pointer based attacks and mitigations*	*Lab 8: Demo on Formatted output security*	*Lab 11: Demo on XSS attacks and remedies*	*Lab 14: Demo on software security analysis and testing tools*
	SLO-2					
S-11	SLO-1	*Cryptographic foibles – random numbers*	*C++ Dynamic Memory Management*	*Recommended Practices, The Security Development Lifecycle*	*File system security principles*	*Software Assurance Initiatives, Activities,and Organizations*
	SLO-2	*Key management issues*	*Common C++ Memory Management Errors*	*Security Training, Requirements*	*File system security processing*	*Government initiatives*
S-12	SLO-1	*Life-cycle of keys*	*Memory Managers*	*Design principles, Implementation considerations*	*Access policies for NFS, SMB, and FTP*	*Private sector initiatives*
	SLO-2	*PKI, Encryption Key Management in Meeting Compliance*	*Heap Overflows and Double-Free Vulnerabilities*	*Verification methods*	*Forceful browsing*	*Secure software Education, training and awareness.*
S-13	SLO-1	*Attacks against the ciphers*	*Double-Free Attacks*	*Metrics and Compliance Reporting*	*Directory traversal*	*Essential Components of an Effective Security Awareness Program*
	SLO-2	*Mitigation strategies in key management*	*Mitigation Strategies for memory errors*	*Static Analysis Security Testing*	*OWASP, CVE, CVSS, CWE, CWSS*	*Implementing Security Education, Training & Awareness*
S14-15	SLO-1	*Lab 3: Demo on cryptosystem key management techniques*	*Lab 6: Demo on C++ memory attacks and mitigations*	*Lab 9: Demo on secure software verification tools*	*Lab 12: Demo on file security*	*Lab 15: study on secure software initiatives and programs*
	SLO-2					

Learning Resources	1. *Michael Howard , David LeBlanc, "Writing Secure Code", Microsoft Press, 2nd Edition, 2003* 2. *Robert C.Seacord, " Secure Coding in C and C++", Pearson Education, 2nd edition, 2013* 3. *David A. Gary McGraw and John Viega, "Building Secure Software: How to Avoid Security Problems the Right Way", Published: September 24, 2001.* 4. *Bryan Sullivan, Vincent Liu, "Web Apllication Security – A Beginner's Guide* 5. *Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, " Software Security Engineering : A guide for Project Managers", Addison-Wesley Professional, 2008* 6. *Ron Ben Natan, "Implementing Database Security and Auditing: A guide for DBAs, Information security administrators and auditors", Published by Elsevier Inc., 2005*

Learning Assessment

	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers

Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
		1. *Mr. Savaridasan, SRMIST, KTR*

Course Code	20ITE559J	Course Name	PENETRATION TESTING AND VULNERABILITY ASSESSMENT	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses	NiL	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the basic of Ethical hacking and terminologies
CLR-2 :	Understand the network,filesystem, system level access
CLR-3 :	To identify security vulnerabilities and weaknesses in the target applications
CLR-4 :	To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
CLR-5 :	To test and exploit systems using various tools.
CLR-6 :	To understand the impact of hacking in real time machines.

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Apply the knowledge Ethical hacking as pentester	2	80	70
CLO-2 :	Identify and design the attackscenario to exploit the target system /network	3	85	75
CLO-3 :	Implement and investigate the procedure of System level hacking	3	75	70
CLO-4 :	Identify , implement and investigate on Wireless penetration testing	1	85	80
CLO-5 :	Identify and investigate the Web vulnerability	1	85	75
CLO-6	Design and implement scanning and network	3	80	70

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	-	H	-	-	-	-	-	-	-	-	-	-	-
H	H	H	H	H	-	-	-	-	-	-	-	M	-	M

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Introduction to Ethical Hacking	Introduction to Scanning	Introduction to Keylogger	Inferential SQL Injection	Introduction to Wireless Pentest –
	SLO-2	Ethics and Legality	Scanning architecture	Keylogger Types	Out of Band SQl Injection	Wifi IEEE 802.11
S-2	SLO-1	Identifying different types of hacking technologies	Scanning Types	Password Hacking Techniques	Introduction to Maintaining Access	WIFI Authentication Modes
	SLO-2	Understanding the different phases involved in ethical hacking – Five stages	Scanning Types	Introduction to Gaining access	Introduction Web Penetration Testing	Types of Wireless encryption
S-3	SLO-1	Types of Teaming	TCP Header	Metasploit	OWASP	Wlan Encryption Flaws

Duration (hour)		15	15	15	15	15
	SLO-2	Non-disclosure agreement Checklist	TCP Connection Process	Metasploit payload	Broken Authentication	WEP
S4-5	SLO-1	Lab 1 : Foot Printing-NMAP	Lab 4: Password Cracking Techniques	Lab 7: ARP / Mac Flooding	Lab 10: Broken Authentication	Lab 13By passing Authentication
	SLO-2					
S-6	SLO-1	Non-disclosure agreement Checklist- II	List TCP Communication	Escalating Privileges	Introduction to Sensitive data exposure and XML External Entities	WPA
	SLO-2	Phases of Hacking	Flag Types	Escalating Privileges	Attack Procedure and Exploit	WPA2
S-7	SLO-1	Open _Source Pentest Methodologie	Understand Banner Grabbing and OS Fingerprinting Techniques	Hiding Files	Introduction toBroken access code	Introduction to access point
	SLO-2	Foot Printing	Introduction to DNS	Double encoding	attack procedure and exploit	Types of AP attacks
S-8	SLO-1	Foot Printing _ procedure	DNS Enumeration	Introduction to Steganography	Introduction XSS	Dos – Layer 1 , Layer 2,
	SLO-2	Foot Printing – Analyzing the output	DNS Records	Types of Steganography	Attack procedure , exploit	DDos Attack
S9-10	SLO-1	Lab 2 Nessus	Lab 5: MetasploitHacking windows 7	Lab 8: Sql Injection	Lab 11: Broken Access code	Lab 14: AP attacks on the WLAN infrastructure
	SLO-2					
S-11	SLO-1	Social Engineering	working of DNS	Countermeasures	Persistent XSS	Client Misassociation
	SLO-2	Social Engineering Types	Types of Domains	ARP Poisoning	Reflection XSS	Wireless hacking methodology
S-12	SLO-1	Social Engineering countermeasures	Types of DNS Servers	MAC Flooding	Dom Based XSS	Wireless Hacking Procedure
	SLO-2	Phishing Attacks	ARP / Keylogging	Introduction to SQL Injection	XSS and its types	Case Study – Investigation onWiFI Traffic in real scenario
S-13	SLO-1	Real time attack – to identify threat and its severity	ARP Header	SQL Injection Types	XSS Discovery	Case Study – Practice on CTF(Capture the 0flag)
	SLO-2	understanding of real time scenario attack as pentester	ARP Spoofing	In Band SQL Injection	XSS Prevention	Report writing as pentester
S14-15	SLO-1	Lab 3: DNS Enumeration,Scanning	Lab 6: : Hiding files , Steganography	Lab 9: Maintain Access	Lab 12: XSS and its types	Lab 15:Wireless Traffic analysis

Learning Resources	
	1. Kali Linux Wireless Penetration Testing Beginner's Guide by VivekRamachandran, Cameron Buchanan,2015 Packt Publishing 2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, SyngressPublicatio 3. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing. 4. Kali Linux 2: Windows Penetration Testing, By Wolf Halton, Bo Weaver , June 2016 Packt Publishing

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
	Understand								
Level 2	Apply	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
	Analyze								
Level 3	Evaluate	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Create								
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
	1.Mr.Ashok Kumar Mohan , Amrita University	*1. Ms. Kirthiga Devi T, SRMIST, KTR*
	2. Ms. Chitra , SSN college of Engineering	

Course Code	20ITE560J	Course Name	MOBILE AND DIGITAL FORENSICS	Course Category	E	Professional Elective	L	T	P	C
							3	0	2	4

Pre-requisite Courses		Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understand the basic of forensic investigation and its procedure, policies on laws in android security
CLR-2 :	Understand the handheld device filesystem
CLR-3 :	Acquire knowledge in investigation procedure and its policies
CLR-4 :	Exploring new aspect in investigation in every aspect of models
CLR-5 :	Understand the role of Investigation guidelines
CLR-6 :	Implement and analyze the evidence to formulate the strategy

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Apply the knowledgemobileforensic investigation	2	80	70
CLO-2 :	Identify and design the attack scenario for mobile forensic	3	85	75
CLO-3 :	Implement and investigate the procedure evolve in mobile forensic investigation	3	75	70
CLO-4 :	Identify, implement and investigate on the imaging	1	85	80
CLO-5 :	Identify and investigate the Seizure models	1	85	75
CLO-6	Design and implement the Examination principles and android security	3	80	70

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design, Research	Modern Tool Usage	Society & Culture	Environment & Sustainability	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	H	-	-	-	-	-	-	-	-	-	M	-	-
H	H	-	-	-	-	-	-	-	-	-	-	M	-	M
H	H	-	-	-	-	-	-	-	-	-	-	-	-	-
H	-	-	H	-	-	-	-	-	-	-	-	-	-	-
H	H	H	H	H	-	-	-	-	-	-	-	M	-	M

Duration (hour)		15	15	15	15	15
S-1	SLO-1	Overview of wireless technologies and security	Cia triad in mobile phones-voice	Mobile phone forensics	Digital forensics: introduction	Digital forensics examination principles:
	SLO-2	Personal area networks, wireless local area networks,	Sms and identification data	Crime and mobile phones, evidences,	Evidential potential of digital devices: closed vs. Open systems	Previewing
S-2	SLO-1	Metropolitan area networks, wide area networks	Interception in gsm:introduction, practical setup and tools,	Forensic procedures,	Evaluating digital evidence potential	Imaging
	SLO-2	Wireless threats, vulnerabilities and security		Files present in sim card, device data,	Device handling and model	Continuity
S-3	SLO-1	Wireless lans, war driving,	Implementation-software and hardware	External memory dump, evidences in memory card, operators systems	Seizure issues	Hashing
	SLO-2					

Duration (hour)		15	15	15	15	15
S 4-5	SLO-1	Lab 1: report writing – for any case study	Lab 4 – android forensic imaging	Lab7 – understanding on various imaging types	Lab 10 - capture the flag in mobile forensic	Lab 13- computing cryptographic hash for an application using tool.
	SLO-2					
S-6	SLO-1	Pda security, cell phones and security	Gsm network service	Android forensics:	Contamination	Seven element security model
	SLO-2					
S-7	SLO-1	Wireless dos attacks, gps jamming, identity theft.	Mobile phone codes	Procedures for handling an android device,	Android data and app security -	Developmental model of digital systems
	SLO-2					
S-8	SLO-1	Digital forensics review-investigative process-	Catalog tricks	Imaging android usb mass storage devices,	Data theft from android devices-	Audit and logs
	SLO-2	Analysis methodologies-tools and techniques	At command set	Imaging types	Encrypted android devices-	Evidence interpretation
S9-10	SLO-1	Lab 2 – review on mobile codes	Lab 5: analyzing case study on mobile phone codes	Lab 8- performing usb operations on smart phones	Lab 11- capture the flag in application oriented	Lab 14- implementing android boot loaders
	SLO-2					
S -11	SLO-1	Report writing	Mobile phone tricks: net monitor	Understanding zero-day exploits	Device identification networked devices	Android rom and boot loaders-android update mechanism
	SLO-2					
S-12	SLO-1	Legacy in ethics, procedures	Sms security issues	Procedure in handling evidence	Corporate mobile security policies and procedures	Evidence locations and it types
	SLO-2					
S-13	SLO-1	War chalking, war flying, common wi-fi security recommendations	Hardware tricks	Logical techniquesphysical techniques	Android software development security strategies	Data content and contextoverview of android devices (phones, tablets, netbooks, etc.)-
S14-15	SLO-1	Lab 3 : managing the evidences on mobile devices	Lab 6- analyzing case study on at command set	Lab 9- create an zero day exploit of android application	Lab 12- combined blackberry/android case	Lab 15- performing android device investigation
	SLO-2					

Learning Resources		
	1. Gregory Kipper, "Wireless Crime and Forensic Investigation", Auerbach Publications, 20072.Iosif	3. Andrew Hoog, " Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 20114.
	2. Androulidakis, " Mobile phone security and forensics: A practical approach",Springer publications, 2012	4. Angus M.Marshall, " Digital forensics: Digital evidence in criminal investigation",John –Wiley and Sons, 2008

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3# (15%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	*20%*	*20%*	*15%*	*15%*	10%	10%	*15%*	*10%*
Level 2	Apply Analyze	*20%*	*20%*	*15%*	*15%*	20%	20%	*20%*	*20%*
Level 3	Evaluate Create	*10%*	*10%*	*20%*	*20%*	20%	20%	*15%*	*20%*
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
	1.Mr.*Ashok Kumar Mohan , Amrita University*	***1.*** *Ms. Kirthiga Devi T , SRMIST, KTR*
	2. Ms. Chitra, SSN college of Engineering	

Course Code	20ITE561T	Course Name	STORAGE MANAGEMENT AND SECURITY	Course Category	E	Professional Elective	L	T	P	C
							3	1	0	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	To explain the basic information storage and retrieval concepts.
CLR-2 :	To understand the issues those are specific to efficient information retrieval.
CLR-3 :	To design and implement a small to medium size information storage and Retrieval system.
CLR-4 :	To implement security issues while storing and retrieving information.
CLR-5 :	To Manage the storage Infrastructure

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking	Expected Proficiency	Expected Attainment
CLO-1 :	Acquire the knowledge of Storage Technology	2	80	85
CLO-2 :	Acquire the process of eifficient information retrieval	2	75	80
CLO-3 :	Design and implement small to medium Information storage and retrieval system	2	85	80
CLO-4 :	Acquire the ability to secure the storage infrastructure	2	80	75
CLO-5 :	Apply the knowledge gained on storage manamagement	2	75	85

Program Learning Outcomes (PLO)															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design,	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
H	H	-	-	H	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
-	H	-	-	H	-	-	-	-	-	-	-	-	-	-
-	H	-	-	H	-	-	-	-	-	-	-	-	-	-

Duration (hour)		12	12	12	12	12
S-1	SLO-1	Information Storage	FC SAN and its components	Business continuity	information security framework	Storage Infrastructure Management
	SLO-2	Evolution of Storage Technology	FC architecture	Information availability metrics	Risk triad	Monitoring Storage Infrastructure
S-2	SLO-1	Core elements of data center	FC SAN topologies and zoning	BC terminologies	Security elements	Monitoring Parameters
	SLO-2	Key characteristics of data center	virtualization in SAN environment	BC planning	Security controls	Alerts
S-3	SLO-1	Application, DBMS, and Host	FC protocol stack	Business impact analysis	Securing the Application Access Domain	Availability Management
	SLO-2	Physical components of connectivity	Types of zoning	Multipathing software	Securing the Management Access Domain	Capacity Management
S-4	SLO-1	Tutorial 1: Calculating the number of disk Required	Tutorial 4: Working of FC Hub and Switches	Tutorial 7: Discussion on virtual LAN and virtual SAN. EMC Atmos	Turotial 10: Discussion on EMC Replication products	Tutorial 13: Discussion on Monitoring mechanism
	SLO-2					
S-5	SLO-1	Storage connectivity protocols	Block-level storage virtualization and virtual SAN	Backup granularities	Securing Backup, Replication, and Archive Domain	Performance Management

Duration (hour)		12	12	12	12	12
	SLO-2	*Disk drive components, addressing, and performance*	*IP SAN protocols, components, and topology*	*Backup and recovery operations*	*Security threats in each domain*	*Security Management*
S-6	SLO-1	*Enterprise Flash drives*	*FCoE protocol, components, and topology*	*Data deduplication*	*Controls applied to reduce the risk in each domain*	*Reporting*
	SLO-2	*Host access to storage and direct-attached storage*	*Drivers for FCoE*	*Common backup topologies*	*SAN security implementations*	*Storage Multitenancy*
S-7	SLO-1	*RAID Implementation methods*	*Components of FCoE network*	*Backup in NAS environment*	*SAN Security Architecture*	*Storage management Challenges*
	SLO-2	*RAID array components*	*FCoE frame mapping*	*Backup Targets*	*NAS security implementations*	*Storage Management Initiative*
S-8	SLO-1	*Tutorial 2 : Reconfigure storage for accounting application for high availability*	*Tutorial 5: EMC Connectrix Family and EMC Celera*	*Tutorial 8: Discussion on RTO and RPO with examples*	*Tutorial 11: Discussion on security threats for Storage management*	*TUtiral 14: Discussion in lifecycle management of ISM*
	SLO-2					
S-9	SLO-1	*RAID techniques*	*Converged Enhanced Ethernet (CEE)*	*host-based, array-based, and network-based local replication technologies*	*Types of ACL's*	*Challenges in Managing Information*
	SLO-2	*RAID Levels*	*NAS, its benefits, and components*	*local replication in virtualized environment*	*Kerberos*	*Information Lifecycle Management*
S-10	SLO-1	*Components of an Intelligent Storage System*	*NAS file-sharing protocols*	*Mirroring of a virtual volume*	*IP SAN security implementations*	*Benefits of ILM*
	SLO-2	*Cache management and protection techniques*	*NAS implementations*	*Replication of virtual machines*	*Security in Cloud Environments*	*Storage Tiering*
S-11	SLO-1	*Storage provisioning and ISS implementation*	*Object-based Storage*	*Remote Replication Overview*	*Security concerns*	*Inter and Intra Tiering*
	SLO-2	*Types of intelligent storage systems*	*Unified Storage*	*Remote Replication Technologies*	*Security measures*	*Cache Tiering*
S-12	SLO-1	*Tutorial3: Allocating and Assigning LUNs*	*Tutorial 6: CAS in Healthcare application*	*Tutorial 9: Discussion on key design consideration for Backup and Restore*	*Tutorial 12: Discussion on security solutions for storage management*	*Turial 15: Discussion on tiering mechanism*
	SLO-2					

Learning Resources	1. *Information Storage and Management: Storing, Managing, and Protecting Digital Information, EMC Corporation* 2. *John Chirillo, Scott Blaul, "Storage Security: Protecting SAN, NAS and DAS", Wiley Publishers, 2003* 3. *David Alexander, Amanda French, David Sutton,"Information Security Management Principles" The British Computer Society, 2008*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	40%	-	30%	-	20%	-	25%	-
Level 2	Apply Analyze	40%	-	30%	-	40%	-	40%	-
Level 3	Evaluate Create	20%	-	40%	-	40%	-	35%	-
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1.Mr.Vivekanandan ,Nokia Technology Specialist, anandanviv1@gmail.com		*1. Dr. J. Godwin,Assistant Professor, Department of IT, SRMIST, KTR*
2.Mr.SanthoshKumar.S,Associate Consultant,TCS, santhosh.sansoft@gmail.com		

Course Code	20ITE562T	Course Name	APPLIED CRYPTOGRAPHY	Course Category	E	Professional Elective	L	T	P	C
							3	1	0	4

Pre-requisite Courses	Cryptography and Network Security	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understandbasic encryption methods and algorithms, the strengths and weaknesses of encryption algorithms
CLR-2 :	Understand encryption key exchange and management
CLR-3 :	Understand how to deploy encryption techniques to secure data stored on computer systems
CLR-4 :	Understand how to deploy encryption techniques to secure data in transit across data networks
CLR-5 :	To demonstrate best practical deployment of cryptographic technologies

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Acquire the knowledge on the fundamentals of various encryption techniques and algorithms	1	80	85
CLO-2 :	Acquire the ability of key exchange and management	1	75	80
CLO-3 :	Apply the principles of various encryption techniques to securely store data	2	85	80
CLO-4 :	Apply the principles of various encryption techniques to securely data in transit across data networks	2	80	75
CLO-5 :	Acquire the knowledge of various cryptographic technologies	1	75	85

Program Learning Outcomes (PLO)															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research Skills	Team Work	Scientific Reasoning	Reflective Thinking	Self-Directed Learning	Multicultural	Ethical Reasoning	Community	ICT Skills	Leadership Skills	Life Long Learning
H	L	L	M	M	-	H	-	-	-	-	-	-	-	-
H	H	L	-	M	-	H	-	-	-	-	-	-	-	-
H	H	H	H	H	-	H	M	-	-	-	-	-	-	-
H	M	L	-	M	L	H	-	-	-	-	-	-	-	-
H	H	L	-	M	L	H	-	-	-	-	-	-	-	-

Duration (hour)		12	12	12	12	12
S-1	SLO-1	Foundations–Terminology, Steganography, Substitution Ciphers and Transposition Ciphers	Key Length	Information Theory	Pseudo-Random-Sequence Generators	RSA Algorithm
	SLO-2	Simple XOR ,One time Pad, Computer Algorithms, Large numbers,Protocol Building Blocks- Introduction to Protocols Communications Using Symmetric Cryptography	Key Management	Complexity Theory	Stream Ciphers	Pohlig-Hellman - McEliece
S-2	SLO-1	One Way Functions, one way hash functions, Communications using public key cryptography, Digital Signatures, Digital Signatures with Encryption	Electronic Codebook Mode	Number Theory- Number Theory-Prime Numbers, Finding an inverse, Discrete Logarithm, Galois Field	Rivest Cipher 4(RC4) Algorithm	Elliptic Curve Cryptosystems

Duration (hour)		12	12	12	12	12
	SLO-2	*Random and Pseudo random sequence generation key exchange, Authentication and key exchange.*	*Block Replay Cipher Block Chaining Mode*	*Factoring Prime Number Generation*	*Software Optimized Encryption Algorithm (SEAL)*	*Digital Signature Algorithm (DSA)*
S-3	SLO-1	*Intermediate Protocols*	*Stream Ciphers*	***Finite Field***	*Feedback with Carry Shift Registers*	*Gost Digital Signature Algorithm -*
	SLO-2	*Timestamping Services-Subliminal channel-Undeniable digital signatures*	*Self-Synchronizing Stream Ciphers*	*Discrete Logarithms in a Finite Field*	*Stream Ciphers Using FCSRs*	*Discrete Logarithm Signature Schemes*
S-4	SLO-1	*Tutorial 1: Discussion on the various cipher techniques.*	*Tutorial 4: Discussion with case studies on impacts of the various ciphers*	*Tutorial 7:Discussion with case studies on the impact of number theory in cryptography*	*Tutorial 10:A study on various pseudo random sequence generators*	*Tutorial 13: Discussion with case studies on impacts of ECC*
	SLO-2					
S-5	SLO-1	*Advanced Protocols*	*Cipher Feedback Mode Synchronous Stream Ciphers Output-Feedback Mode*	*Data Encryption Standard (DES)*	*Non linear Feedback Shift Registers*	*Ongchnorr*
	SLO-2	*Zero-Knowledge Proofs*	*Counter Mode Choosing a Cipher Mode Interleaving*	***Substitution Box (S-BOX)***	*System-Theoretic Approach to Stream*	*Shamir*
S-6	SLO-1	*Zero-Knowledge Proofs of Identity*	*Block Ciphers versus Stream CiphersChoosing an Algorithm*	*Lucifer Algorithm*	*Cipher Design - Complexity*	*Cellular Automata*
	SLO-2	*Blind Signatures*	*Block Ciphers versus Stream CiphersChoosing an Algorithm*	*Madryga Algorithm*	*Theoretic Approach to Stream*	*Feige-Fiat-Shamir*
S-7	SLO-1	*Identity-Based Public-Key Cryptography*	*Public- Key Cryptography*	*New Data Encryption Standard Algorithm*	*Cipher Design*	*GuillouQuisquater*
	SLO-2	*Oblivious Transfer*	*Symmetric Cryptography*	*GOST Block Cipher(Magma)*	*N- Hash*	*Diffie-Hellman*
S-8	SLO-1	*Tutorial 2: Discussion with case studies on knowledge proof*	*Tutorial 5: Discussion with case studies on impacts of the various block cipher modes.*	*Tutorial 8: Discussion with case studies on the strength of S-BOX*	*Tutorial 11: A survey on the complexity of cipher design*	*Tutorial 14: Discussion on the various protocols*
	SLO-2					
S-9	SLO-1	*Oblivious Signatures*	*Encrypting Communications Channels*	*3 Way Block Cipher, Crab Block Cipher*	*Message Digest(MD4) algorithm*	*Station-to-Station Protocol*
	SLO-2	*Simultaneous Contract Signing*	*Encrypting Data for Storage - Hardware Encryption versus Software Encryption*	*RC5 Block Cipher*	*Message Digest(MD5) algorithm*	*Shamir's Three-Pass Protocol*
S-10	SLO-1	*Digital Certified Mail*	*Compression*	*Double Encryption*	*Message Digest (MD2) algorithm*	*IBM Secret-Key Management Protocol*
	SLO-2	*Simultaneous exchange of secrets*	*Encoding, and Encryption - Detecting*	*Triple Encryption*	*Secure Hash Algorithm (SHA)*	*MITRENET*
S-11	SLO-1	*Esoteric Protocols-Secure Elections, Secure Multiparty Computation*	*Detecting Encryption*	*CDMF Key Shortening*	*Other One- Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms -*	*Kerberos*

Duration (hour)		12	12	12	12	12
	SLO-2	*Anonymous Message –Broadcast, Digital Cash*	*Hiding and Destroying Information.*	*Whitening*	*Message Authentication Codes*	*IBM Common Cryptographic Architecture*
S-12	SLO-1	*Tutorial 3: Discussion with case studies on digital cash*	*Tutorial 6: Discussion with case studies on the hardware /software encryption*	*Tutorial 9: Discussion with case studies on the various RC5 techniques.*	*Tutorial 12: Discussion with case studies on the various MD techniques*	*Tutorial 15: A comprehensive study on the IBM architectures.*
	SLO-2					

Learning Resources		
	1. *Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley & Sons, Inc, 2nd Edition, 1996.*	3. *AtulKahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.*
	2. *Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004*	4. *William Stallings, "Cryptography and Network Security", 3rd Edition, Pearson Education, 2003.*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember / Understand	40%	-	30%	-	20%	-	25%	-
Level 2	Apply / Analyze	40%	-	30%	-	40%	-	40%	-
Level 3	Evaluate / Create	20%	-	40%	-	40%	-	35%	-
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. *Mr.Vivekanandan ,Nokia Technology Specialist, anandanviv1@gmail.com*	1. *Dr.C.M.T.Karthigeyan,(A.P-CSE),c.m.t.karthikeyan@gcebargur.ac.in*	1. *Ms.Sujatha.G, Assistant Professor,Dept of IT, SRMIST, KTR*
2. *Mr.SanthoshKumar.S,Associate Consultant,TCS, santhosh.sansoft@gmail.com*		2. *Ms.Saveetha.DAssistant Professor, Dept of IT, SRMIST, KTR*

Course Code	20ITE642T	Course Name	RISK ASSESSMENT AND SECURITY AUDIT	Course Category	E	Professional Elective	L	T	P	C
							3	1	0	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:
CLR-1 :	Understandthefundamental knowledge about Information Risk.
CLR-2 :	Understandthevarious analysis on Information Risk Assessment.
CLR-3 :	Understandthe demand for IS Audit.
CLR-4 :	UnderstandtheIT audit and its activities.
CLR-5 :	Understandthetechniquesforimplementing security in audit.

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Acquire the knowledge on the fundamentals of Risk assessment	1	80	75
CLO-2 :	Acquire the ability to apply various techniques for data collection	1	85	75
CLO-3 :	Utilize the principles of data analysis	2	75	70
CLO-4 :	Acquire the ability to apply IS audit	3	85	70
CLO-5 :	Apply the knowledge gained on auditing methodologies	3	85	70

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Disciplinary Knowledge	Critical Thinking	Problem Solving	Analytical Reasoning	Research Skills	Team Work	Scientific Reasoning	Reflective Thinking	Self-Directed Learning	Multicultural Competence	Ethical Reasoning	Community Engagement	ICT Skills	Leadership Skills	Life Long Learning
H	M	M	M	-	L	L	M	-	-	M	-	-	-	-
H	M	M	M	L	M	L	L	-	-	H	L	-	L	L
H	L	M	L	L	L	L	M	-	-	M	-	-	L	L
H	M	M	M	L	M	L	M	-	-	H	L	-	M	M
H	M	M	M	L	M	L	M	-	-	M	L	-	-	L

Duration (hour)		12	12	12	12	12
S-1	SLO-1	Introduction to Risk	Introduction to data collection	Introduction to data analysis	Demand for IS audit	Detailing Information Security Audit
	SLO-2	Elements of risk	Planning – the essential element	Compiling Observations	Auditor Role	Purpose of IS Audit
S-2	SLO-1	Information Security Risk Assessment Overview	The Sponsors	Risk assessment frameworks overview	Auditee Role	Expectation from IS Auditor
	SLO-2	Information Risk Assessments Activities	Characteristics of a good project sponsor	Compiling Observations from Organizational Risk Documents	Process of auditing information system	Steps to Conduct IS Audit
S-3	SLO-1	Risk Assessments and the Security Program	The project team	Format to collect your observations.	Preplanning the audit	Classification of Audit, Traditional Audit
	SLO-2	Drivers	Factors that decide upon the size of the project team	List of the documents to encounter	Audit process	Difference Between Audit and Assessment
S-4	SLO-1	**Tutorial 1:** Activities in a Risk Assessment	Tutorial 4: Generate project team	**Tutorial 7:** System Risk Computation Impact Analysis Scheme	Tutorial 10:Perform an audit risk assessment	Tutorial 13: Review ISACA Auditing Standards
	SLO-2					

Duration (hour)		12	12	12	12	12
S-5	SLO-1	*Laws*	*Data collection mechanisms*	*Threat Catalog*	*Perform audit*	*Relationship Between Auditor, Auditee and Client;*
	SLO-2	*Regulations*	*Collectors and Containers*	*List of threat catalogs that can be used as references*	*Hierarchy of internal controls*	*Their Duties*
S-6	SLO-1	*Primary Information Security Risk Assessment "Drivers"*	*Executive interviews*	*Sample Threat Catalog*	*Gathering audit evidence*	*SLA Introduction*
	SLO-2	*Threat Source Leveraging a Vulnerability*	*Questionnaire*	*Vulnerability Catalog*	*Conducting audit evidence*	*SLA Components*
S-7	SLO-1	*Federal Information Security Management Act of 2002 (FISMA)*	*Document requests*	*Vulnerability Catalog types*	*Reporting audit evidence*	*Auditing Firm Organizational Chart*
	SLO-2	*Gramm-Leach-Bliley Act (GLBA)*	*List of documents for the assessor*	*Documentation process*		*Auditing Firm functionalities*
S-8	SLO-1	*Tutorial 2: Information Security Risks Assessment*	*Tutorial 5: Conducting mock executiveinterviews*	*Tutorial 8: Building the catalog*	*Tutorial 11: Documenting the audit evidence*	*Tutorial14: Auditing Document Preparations*
	SLO-2					
S-9	SLO-1	*Health Insurance Portability and Accountability Act (HIPAA)*	*IT Assets inventory*	*Threat Vulnerability Pairs*	*Strategy planning for organizational control*	*Policy Vs Procedures Standard Vs Guideline*
	SLO-2	*ISO 27001*	*Asset Scoping*	*Sample Threat and Vulnerability Pairs*	*Issues register*	*Basic Types of Measurement Metrics*
S-10	SLO-1	*ISO 27005*	*Asset Scoping - Requirements*	*Confidentiality*	*Risk Assessment tools*	*Members of Auditing Committee*
	SLO-2	*Risk Assessment Frame work*	*Techniques involved in asset scoping*	*Confidentiality Determination Matrix*	*Distinct types of risk tools*	*Skills Matrix, Example*
S-11	SLO-1	*Risk Assessments and the Security Program*	*Profile survey*	*Analyzing Confidentiality Determination Matrix*	*Planning*	*Audit Evidence, Examples*
	SLO-2	*Practical Approach.*	*Control survey*	*Developing Sample Confidentiality Determination Matrix*	*Performance*	*Direct and Indirect Evidence*
S-12	SLO-1	*Tutorial 3: Case study: Security Risk Management in Healthcare*	*Tutorial 6: Crisis Management Case Study*	*Tutorial 9: Fraud & Internal Security Case Study*	*Tutorial 12: Hotel & Hospitality Case Study*	*Tutorial 15: Generating sample Evidence Life Cycle*
	SLO-2					

Learning Resources	
	1. *MarkTalabis, "Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis", Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.*
	2. *David L. Cannon, "CISA Certified Information Systems Auditor Study Guide", John Wiley & Sons, ISBN: 978-0-470-23152-4, 2009.*
	3. *RobertJ, Schalkoff,"PatternRecognition:Statistical,StructuralandNeuralApproaches", John Wiley&SonsInc.,New York, Reprint2014.*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	40%	-	30%	-	20%	-	25%	-
Level 2	Apply Analyze	40%	-	30%	-	40%	-	40%	-
Level 3	Evaluate Create	20%	-	40%	-	40%	-	35%	-
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. *Ms.SaliniKotari, Associate consultant, KPMG, Chennai.*		1. *Ms.C.Fancy,Assistant Professor , Department of ITSRMIST, KTR*
2. *Mr.VishwaPrasath.T.S. Security Analyst, Crossbow Labs, Bangalore.*		2. *Mr.Arivazhagan, Assistant Professor , Department of SRMIST, KTR*

Course Code	20ITE643T	Course Name	CYBER LAW AND ETHICS	Course Category	E	Professional Elective	L	T	P	C
							3	1	0	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Information Technology	Data Book / Codes/Standards	Nil		

Course Learning Rationale (CLR):	The purpose of learning this course is to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLR-1 :	Understand the basic information on Cyber Security			
CLR-2 :	Be aware about the basics of Cyber Law and its related issues			
CLR-3 :	Understandtheissues those are specific to amendment rights			
CLR-4 :	Understandtheknowledge on copyright issues of software			
CLR-5 :	Understandtheethical laws of computer for different countries			

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLO-1 :	Gain knowledge on Cyber Security	2	80	85
CLO-2 :	Obtain the basics of Cyber Law and its related issues	2	75	80
CLO-3 :	Utilize the issues which are pertinent to amendment rights	2	85	80
CLO-4 :	Acquire the knowledge on copyright issues of software	2	80	75
CLO-5 :	Apply the ethical laws of computer for various countries	2	75	85

Program Learning Outcomes (PLO)														
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Engineering Knowledge	Problem Analysis	Design & Development	Analysis, Design,	Modern Tool Usage	Society & Culture	Environment &	Ethics	Individual & Team Work	Communication	Project Mgt. & Finance	Life Long Learning	PSO - 1	PSO - 2	PSO – 3
H	-	-	-	-	-	-	-	-	-	-	-	-	-	-
-	H	-	H		-	-	-	-	-	-	-	-	-	-
-	-	H	-	-	H	-	-	-	-	-	-	-	-	-
-	-	-	-	H	-	-	-	-	-	-	-	-	-	-
-	-	-	-	H	H	-	H	-	-	-	-	-	-	-

Duration (hour)		12	12	12	12	12
S-1	SLO-1	Introduction to Cyber Law	Cyber Security – Private Ordering Solutions	Introduction to Intellectual Property Rights	Duty of Care	Introduction to Ethics
	SLO-2	Introduction to Cyber Law	Network Responses to Threats	Intellectual Property Rights-Significance	Negligence	Significance of Ethics
S-2	SLO-1	Cyber Ethics	The Dark side of Private Ordering	Internet Infringement	Negligent Misstatement	Legal Developments – 1990 to 1992
	SLO-2	Awareness about Cyber Ethics	Evolution of Private Legal Systems	Defending the Internet	Equipment Malfunctions	Legal Developments – 1993 to 1995
S-3	SLO-1	Need for Cyber Law	Jurisdiction for global Cyber security	Fair Use	Procedural Issues	Legal Developments – 1996 to 1998
	SLO-2	Applications of Cyber Law	Global Cyber terrorism	Fair Use	Electronic Contracts	Legal Developments – 1998 to 2000
S-4	SLO-1	Tutorial 1: Discussion of Cyber Threat case studies	Tutorial 4: Analyse types of cybercrimes such as Cyber Stalking, Spamming	Tutorial 7: Explore clauses in ISO27001 and ISO27002	Tutorial 10: Explore Network monitoring tools	Tutorial 13: Analyse Ethical Hacking and its tools
	SLO-2					
S-5	SLO-1	Introduction - Cyber Security	Introduction to Copyright	Criminal Liability	Public Key Encryption	Cyber Security and Society
	SLO-2	How Critical is Cyber Security	Copyright - Sources of Risk	Criminal Liability	Digital Signatures	Examples

Duration (hour)		12	12	12	12	12
S-6	SLO-1	*Cyber Security Problems*	*Subject Matter of Copyright*	*Trademarks*	*Utah Digital Signature Act*	*Security in Cyber Laws*
	SLO-2	*Private Vs Social Incentives*	*Pirates*	*Famous Trademarks*	*Proposed Encrypted Communications Privacy Act of 1996*	*Hacking, Denial-of-Service Attacks, Electronic theft*
S-7	SLO-1	*Solution to Cyber Security Issues*	*Internet Infringement*	*Defamation*	*Misappropriation of Information*	*Corporate Governance*
	SLO-2	*Difference between Computer & Network Security*	*Copyright – Email*	*Money Talk Scenario*	*ProCD – Case Study*	*Investigatory and Police Powers*
S-8	SLO-1	*Tutorial 2: Compare Cyber attack classification - Insider and External attacks*	*Tutorial 5: Explore Cyber crime - Real time cases*	*Tutorial 8: Case Study-Money Talk Scenario*	*Tutorial 11: Discussion on Cyber resilience planning in an organisation*	*Tutorial 14: Discussion about Case study on Cyber security in society*
	SLO-2					
S-9	SLO-1	*Intervention Strategies – Redundancy*	*Fair Use*	*Privacy*	*Civil Rights*	*General Law and Cyber Law – Analysis*
	SLO-2	*Peer Production of Survivable Critical Infrastructures*	*First Amendment*	*Common Law Privacy*	*Civil Rights – Case Study*	*General Law and Cyber Law – Analysis*
S-10	SLO-1	*Examples*	*Software Rental*	*Constitutional Law*	*Introduction to Tax*	*Case Study – Open Source Paradigm*
	SLO-2	*Intervention Strategies - Diversity*	*Postings*	*Federal Statutes*	*Tax Procedures for Online*	*Case Study – The Military Paradigm*
S-11	SLO-1	*Intervention Strategies – Autarchy*	*Criminal Liability*	*Anonymity*	*Records*	*Case Study – The Information-Sharing Paradigm*
	SLO-2	*Cost of Engineering Heterogeneity*	*First Amendments, Losing Data*	*Technology Expanding Privacy Rights*	*Evidence*	*Case Study – The Public Domain*
S-12	SLO-1	*Tutorial 3: A comprehensive study on types of malwares*	*Tutorial 6: Case Study - Software Rental*	*Tutorial 9: Analyse Cyber Security Audit*	*Tutorial 12: Explore Cyber security initiatives of India*	*Tutorial 15: Comparison on legal aspects across India, US and UK*
	SLO-2					

Learning Resource	1. *Jonathan Rosenoer, "Cyber Law: The Law of the Internet", Springer-Verlag, 1997.* 2. *Mark F Grady, Francesco Parisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006.* 3. *Salvatore J. Stolfo, Steven M. Bellovin, ShlomoHershkop, AngelosKeromytis, Sara Sinclair, Sean W. Smith, "Insider Attack and Cyber Security – Beyond the Hacker", Springer, 2008* 4. *New Jersey division of consumer affairs, "Cyber Security Handbook".* 5. *India: Cybersecurity 2020, ICLG.com*

Learning Assessment									
	Bloom's Level of Thinking	Continuous Learning Assessment (60% weightage)						Final Examination (40% weightage)	
		CLA – 1 (20%)		CLA – 2 (25%)		CLA – 3 (15%)#			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember Understand	40%	-	30%	-	20%	-	25%	-
Level 2	Apply Analyze	40%	-	30%	-	40%	-	40%	-
Level 3	Evaluate Create	20%	-	40%	-	40%	-	35%	-
	Total	100 %		100 %		100 %		100 %	

CLA – 3 can be from any combination of these: Assignments, Seminars, Tech Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, and Conf. Paper etc.

Course Designers		
Experts from Industry	Experts from Higher Technical Institutions	Internal Experts
1. Mr. Ganesh Subramaniam, CEO & Principal Consultant, Competence Consulting	*1. Dr. A. Subashree, Sri Ramachandra Institute of Higher Education and Research, Faculty of Management*	*1. Mr. P.Gouthaman, SRMIST, KTR*
	2. Dr. M. G. Bhaskar, SRMIST	