WIRELESS AND MOBILE SECURITY
(ELECTIVE – II)

Course Code: 15CS2216

L	P	C
3	0	3

Pre requisites: Mobile Computing.

Course Outcomes:
By the end of the course Students will

CO1: Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.

CO2: Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks.

CO3: Have a broad knowledge of the state-of-the-art and open problems in wireless and mobile security, thus enhancing their potential to do research or pursue a career in this rapidly developing area.

CO4: Learn various security issues involved in cloud computing.

CO5: Learn various security issues related to GPRS and 3G.

UNIT I (10-Lectures)

Security Issues in Mobile Communication**:** Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security.

UNIT II (10-Lectures)

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and

Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT III (10-Lectures)

Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications, GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security and authentication Solutions.

UNIT IV (10-Lectures)

Application Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions.

Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, Some of the security solutions for UC.

UNIT V (10-Lectures)

Data Center Operations - Security challenge, implement "Five Principal Characteristics of Cloud Computing, Data center Security Recommendations Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards.

TEXT BOOKS:

1. Pallapa Venkataram, Satish Babu: "Wireless and Mobile Network Security", 1st Edition, Tata McGraw Hill, 2010.
2. Frank Adelstein, K.S.Gupta: "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.

REFERENCES:

1. Randall k. Nichols, Panos C. Lekkas: "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. Bruce Potter and Bob Fleck: "802.11 Security", 1st Edition, SPD O'REILLY 2005.
3. James Kempf: "Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols", 1st Edition, Cambridge University Press, 2008.