

MITHRAVINDHU KOTHAPELLY

Phone: 8712107307 | Email: kothapellymithravindhu@gmail.com

LinkedIn: [linkedin.com/in/mithravindhu](https://www.linkedin.com/in/mithravindhu) | Location: Bengaluru, Karnataka, India.

EDUCATION

Tata Strive | *Bengaluru* 03/2025
Cyber Security

Manpower Development College | *Hyderabad* 2024
Master of Computer Applications

CORE COMPETENCIES

- **Cybersecurity concepts:** Vulnerability Assessment, Risk Assessment and Management, SAST & DAST, VAPT, OWASP Top 10, Incident Response, CIA.
- **Cryptography:** AES, RSA, 3DES, Diffie-Hellman Key Exchange.
- **Networking:** OSI Model, TCP/UDP, IP Address, MAC Address, Ports & Protocols.
- **Network Security:** VPN, FIREWALL, SSL/TLS, VPN, PROXY.
- **Security Tool:** Nmap, Burp Suite, Metasploit, Nessus, Wireshark.
- **Operating Systems:** Kali Linux, Windows.
- **Web Technology:** HTML

PROJECTS

Network Intrusion Simulation

- Built a 3-host network with 10 pre-planted vulnerabilities (e.g., weak credentials) to test defenses.
- Launched 5 MITM attacks using arpspoof and bettercap, capturing 100+ HTTP packets in real-time.
- Investigated traffic with Wireshark and SSL/TLS settings with sslscan, detecting 3 certificate issues.
- Strengthened security by applying Burp Suite brute force on payloads, reducing risks by 20%.

Enhanced Privacy-Aware Authentication for Mobile Cloud Computing

- Developed 1 privacy-aware authentication scheme leveraging identity-based signatures for secure mobile cloud services, efficiently implemented.
- Engineered protocol design to protect user privacy and prevent unauthorized access in mobile cloud computing.
- Optimized computation and communication overhead, reducing overall processing time and cost by 20% substantially.
- Validated protocol performance via extensive simulations, demonstrating improved efficiency and robust privacy preservation outcomes by 15%.

Web Application Penetration Testing – SSRF (Server-Side Request Forgery)

- Conducted security assessments on web applications to identify and exploit SSRF vulnerabilities.
- Used Burp Suite and proxy tools for penetration testing and traffic interception.
- Analysed HTTP requests to detect server-side misconfigurations and unauthorized data access.
- Provided detailed remediation steps to developers for fixing SSRF vulnerabilities and improving security posture.

CERTIFICATIONS

- Fortinet Certified Associate in Cyber Security | 2025
- Cisco Networking Basics | 2025