SATHISHKUMAR P

CONTACT

+91 9585879853 | sathish292003@gmail.com | https://github.com/MrsathishKumar

https://www.linkedin.com/in/sathishkumar-p-224156332/

Portfolio: https://mrsathishkumar.github.io/Myprofile/portfolio

CAREER OBJECTIVE

Aspiring Cybersecurity Analyst and Software Developer with A Strong Foundation in Programming, Secure Coding, And System Protection. Seeking An Entry-Level Position Where I Can Apply My Technical Skills to Develop Innovative Software Solutions While Ensuring Security. Eager To Learn, Grow, And Contribute to The Success of The Organization.

EDUCATION

MSC - COMPUTER SCIENCE "Alagappa University, Karaikudi, Tamil Nadu".

2023 - 2025 | CGPA: 7.10.

BSC – COMPUTER SCIENCE "Government Arts and Science College of Tharagampatty, Karur, Tamil Nadu".

2020 - 2023 | CGPA:7.40.

HSC -Government Higher Secondary School, Palaviduthi, Karur. Tamil Nadu.

2019 – 2020 | Percentage: 65%.

SSLC-RC Higher Secondary School, Periya Anaikkaraipatty, Trichy. Tamil Nadu.

2017 – 2018 | Percentage: 86%.

EXPERIENCE

CYBER SECURITY TRAINER | INTERNSHIP
CSUITE TECH LABS.
Jan 2025 - Mar 2025 .
Coimbatore, Tamil Nadu, India.

SMT - AXI OPERATOR
Nokia Network private limit, Chennai.
Sep 2025 -Now Working…

TECHNICAL SKILLS

FRONTEND: HTML | CSS | React JS. LANGUAGES: Advance Java | Functional Programming Python | SQL.

BACKEND: Node.js | PHP. DATABASES: MongoDB | MYSQL | PostgreSQL.

CYBER SECURITY: VAPT | Malware Analysis | SIEM Security | Kali Linux | Social Engineering Tools | Forensics Tools | Networking and Hardware.

SOFT SKILLS

- Adaptability & Flexibility | Time Management and Good communication | leadership & decision making

CERTIFICATION & PARTICIPATIONS

- Cyber5w | Digital Forensic.
- Basant Technology | Core Java (Virtual).
- Nove Tech | Cybersecurity, AI & IOT (Virtual).
- CAPPRICIOSEC UNIVERSITY | Cyber Warrior Participations (Virtual).
- Conference Participation | Blockchain, IOT, Recent Trends in Computer Science, Cyber Security.

PROJECT

ADVANCED PERSISTENT THREAT (APT) DETECTION USING HONEYPOT

Developed Advanced Persistent Threat (APT) Honeypot Systems Integrating SSH, FTP, And Camara Traps with ELK Stack Dashboards to Capture, Analysis, And Visualize Attacker Behaviour in Real Time. Implemented Deception Techniques, Session Logging, IP Geolocation, And Automated Alerts to Enhance Threat Intelligence, Forensic Analysis, And Proactive Cybersecurity Defence.

USB MALWARE TOOLS

The USB Malware Detection System Is a Cybersecurity Tool Designed to Enhance Device Security by Scanning Wired and Wireless Connections, Including USB, LAN, And Bluetooth Devices, For Potential Malware Threats. The System Provides a One-Time Scan Functionality and Includes a Graphical User Interface (GUI) For User-Friendly Interaction.

IP BLOCKER AND NMAP SCANNER BROWSER EXTENSION

This Projects was Enhances Security by Allowing Users to Block Malicious Ips in Real Time and Manage Blacklists, While Also Providing Reconnaissance Capabilities to Scan Open Ports and Services. Together, They Help Prevent Unauthorized Access, Identify Vulnerabilities, And Strengthen Proactive Defence.

ANTI-KEYLOGGER DETECTION SYSTEM

The Windows Keylogger and Anti-Keylogger Detection System Encompasses Both the Offensive and Defensive Aspects of Cybersecurity. This Project, Provides A Dual-Function Platform That Includes a Keylogging Module for Capturing and Analysis User Keystrokes, And an Anti-Keylogger Module That Detects and Mitigates Potential Keylogging Threats.

AI-POWERED FRAUD DETECTION SYSTEM FOR ONLINE TRANSACTION

This Project Development of a Web-Based Fraud Detection System That Leverages Machine Learning Techniques to Identify Suspicious Financial Transactions. With The Digital Payments and Online Banking, Financial Fraud Has Become Increasingly Sophisticated. Detecting Fraudulent Activities in Real-Time Is Crucial to Protect Users and Financial Institutions from Potential Losses.