Madhav Mishra

9301702256 | madhavmishra663@gmail.com | linkedin.com/in/madhav-mishra-24879a250 | github.com/madhav663

Education

K.V No.1 GCF — Jabalpur, M.P
PCM with Computer Science — *July 2020 – Aug 2022*

Vellore Institute of Technology, Bhopal — Bhopal, M.P
Integrated M.Tech in Computer Science and Engineering (Cyber Security) — *Oct. 2022 – July 2027*

Research Work

Undergraduate Researcher — Hybrid Dual-Signature Scheme (HDSS) — Feb 2025 – Present
VIT Bhopal University — *Bhopal, India*

- Proposed and implemented a **Hybrid Dual-Signature Scheme (HDSS)** combining Falcon and SPHINCS+ post-quantum algorithms to strengthen blockchain and IoT security against quantum adversaries.
- Developed a proof-of-concept Go implementation for key generation, signing, verification, and benchmarking against RSA, ECDSA, and individual PQC schemes.
- Designed an experimental benchmarking framework to evaluate signature size, signing/verification time, and tamper resistance on real-world blockchain/IoT datasets.
- Authored a research paper presenting the HDSS architecture, security analysis, and future deployment strategy for quantum-resilient decentralized systems.

Projects

Secure Automated Grading System | *Python, Golang, Docker, Jenkins* — Dec 2024–April 2025

- Built Dockerized sandbox environments for safe code execution, eliminating cross-container exploits.
- Integrated Jenkins CI/CD pipeline with static/dynamic analysis tools, detecting 92% of common injection flaws before deployment.
- Reduced manual grading workload by 70% and decreased deployment errors by 45% through automation.

Post-Quantum Web 3.0 Security Research | *Python, Golang* — Feb 2025 – Present

- Implemented PQC-based cryptographic models, strengthening blockchain transaction verification against quantum attacks.
- Improved resilience of decentralized identity systems by ∼40% compared to baseline elliptic curve approaches.
- Simulated quantum-safe protocols in IoT and smart finance environments, achieving sub-200 ms verification latency.

Health Menta (Secure Health Data Platform) | *React, Python, MongoDB* — Feb 2025

- Developed OCR-based prescription system with AES-256 encryption for patient data storage and TLS-secured transmission.
- Hardened APIs using JWT authentication and OWASP-recommended input validation, mitigating >80% of common web vulnerabilities.
- Reduced prescription processing time by 35% and enhanced compliance-readiness for HIPAA-like data protection standards.

Technical Skills

- **Languages:** Python, Golang, SQL, C++, JavaScript , Bash
- **Frameworks & Libraries:** Flask, FastAPI, Django, Node.js, Express.js, TensorFlow, PyTorch, Pandas, NumPy, Scikit-learn,Gin,Gorilla Mux
- **Security Tools:** Wireshark, Nmap, Burp Suite, Metasploit, Kali Linux, OWASP ZAP, Nessus, Nikto, sqlmap
- **DevSecOps:** Secure CI/CD Pipelines, SAST/DAST (SonarQube, OWASP Dependency-Check), Container Hardening, Kubernetes RBAC, Docker, Jenkins, GitHub Actions