Atharva Devendra Gajbe

☎ +49 1622879983 ✉ gajbeatharva2000@gmail.com in linkedin.com/in/atharva-gajbe-50a2571aa

github.com/Atharvagajbe

OBJECTIVE

Passionate and detail-oriented Computer Science professional with a solid academic background and hands-on experience in blockchain technology, cybersecurity, and secure systems development. Demonstrated expertise in designing and implementing innovative blockchain-based solutions to ensure data integrity, confidentiality, and tamper-proof transmission — notably through the development of a secure examination paper distribution system. Adept at leveraging technologies such as smart contracts, encryption, and vulnerability assessment tools to address modern security challenges. Known for a strong problem-solving mindset, collaborative approach, and eagerness to contribute to impactful projects in dynamic, fast-paced environments. Currently pursuing a Master's in Applied Computer Science to deepen technical expertise and drive the next generation of secure, decentralized applications.

EDUCATION

Master of Science in Applied Computer Science *2025 – Present*
SRH University Heidelberg, Germany [DE]

Bachelor of Technology in Computer Technology *2018 – 2022*
Yeshwantrao Chavan College of Engineering, Maharashtra Nagpur [IN]

HSC, Shri Shivaji Science, Maharashtra Nagpur [IN] *2016 - 2018*

SSC, Narayana Vidyalayam, Maharashtra Nagpur [IN] *2007 - 2016*

PROFESSIONAL EXPERIENCE

Security Analyst – Cognizant (Google Play Protect) *2022–2025*

- Worked onsite at Google with a 500+ member team to identify and eliminate malware in Android/iOS apps.
- Developed patches for bugs and analyzed obfuscated code to improve application performance.
- Utilized tools like FRIDA and Objection to reverse-engineer APKs and detect suspicious activity.
- Collaborated cross-functionally with QA and development teams to integrate secure coding practices.

Technical Team Lead – TEDx YCCE *2022*

- Led a tech team of 100+; managed software setups, live streaming, and internal portal security.
- Designed a centralized inventory system for equipment tracking and access management.
- Oversaw digital ticketing and participant login system development for smooth registration flow.

Jr. VAPT Auditor – Crypto Forensic Technologies *2022*

- Assisted cybersecurity investigations and cloud infrastructure revamp for major banking institutions.
- Performed reconnaissance, vulnerability scans, and penetration tests to assess risk exposure.
- Documented security gaps and submitted detailed reports with actionable remediation strategies.

Business Development Manager – Motorodi *2019*

- Managed frontend infrastructure and server data flow for customer-facing web solutions.
- Initiated cold calls/emails and built 25+ strong B2B relationships within a year.
- Conducted market analysis to identify local partnership opportunities and growth strategies.

TECHNICAL SKILLS

- **Languages:** Python, Java, Solidity, Bash
- **Blockchain:** Ethereum, Hyperledger, Smart Contracts
- **Tools & Frameworks:** Git, Docker, Kubernetes, Node.js, FRIDA, Objection, Kali Linux, Burp Suite, Metasploit, Wireshark, Nmap, OWASP ZAP, Terraform,
- **Concepts:** Cybersecurity, Data Encryption, VAPT, Reconnaissance, Bug Bounty, Infosec, Reverse Engineering, Threat Modeling, Incident Response, Cloud Security, Network Security, Cryptography
- **Databases:** SQL, NoSQL (MongoDB, Redis), PostgreSQL
- **Cloud Platforms:** AWS (EC2, S3, Lambda, IAM), Google Cloud Platform (GCP),
- **Operating Systems:** Linux (Ubuntu, Debian, CentOS, Kali ,Arch), Windows, macOS

PROJECTS

- **Blockchain-Based Exam Paper Transmission** – Secure blockchain system with encryption to prevent unauthorized access.
- **Scanner-Master** – Network scanner that detects connected devices and displays IP/MAC addresses.
- **Server-Side Template Injection** – Demonstrated SSTI exploitation leading to potential remote code execution.
- **PHP Web Shell** – Lightweight web shell for executing Unix commands remotely.
- **Keylogger** – Captures and logs keystrokes for security research.
- **Phishing Framework** – Simulates phishing attacks for cybersecurity testing.

RESEARCH PAPERS

Blockchain Based Solution for Secured Transmission of Examination Paper
The increasing reliance on online examinations, especially post-COVID-19, highlights the critical need for secure data transmission, addressing trust and transparency concerns. Blockchain technology offers a solution by providing data privacy and integrity through cryptographic validation and smart contracts, eliminating the need for third-party involvement in exam paper transmission.
IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC) Year: 2022 — Conference Paper — Publisher: IEEE

Building Customized Browser Extension Outlining the risks and existing solutions for Third-Party Extensions
Browser extensions, while enhancing user experience and productivity, pose significant security and privacy risks due to their access to sensitive user data. Developed by third parties, these extensions can be malicious, necessitating a focus on secure technologies to mitigate potential threats.
[Under Publication at ICACT : International Conference on Advanced Communications Technology 2025]

LANGUAGES

- **E**nglish (Fluent)
- **G**erman (Conversational)
- **M**arathi (Native)
- **H**indi (Native)
- **S**anskrit (Native)