Research Statement

Dr. Vishal S. Badgujar

Department of Information Technology, A.P. Shah Institute of Technology,
Mumbai University, Thane (West)-400615, Maharashtra, India

Mobile: +91-7709933639

Email: vishalbadgujar4@gmail.com; vsbadgujar@apsit.edu.in

Website: https://www.vishalbadgujar.in

My Approach to Research

My research interests lie at the intersection of Cybersecurity, Artificial Intelligence and Machine Learning, Open-Source Technologies, DevOps, Cloud Computing, and Big Data Analytics. My research objective is to develop intelligent, scalable, and practically deployable approaches for identifying, analyzing, and mitigating emerging cybersecurity threats. I am particularly interested in combining artificial intelligence with behavioral analysis, risk assessment, and open-source security architectures to develop security solutions that are adaptive to evolving threat environments.

My research journey has evolved from a broader interest in computer and network security toward a focused research agenda in AI-driven cybersecurity and risk analysis. My PhD doctoral research in Computer Engineering at the University of Mumbai focuses on Risk Level Analysis of AI-Based Open-Source Architecture, under the supervision of Dr. Chandrashekhar Raut. This work reflects my broader objective of understanding how intelligent and open-source computing architectures can be systematically evaluated for security risks and how machine learning can support proactive security decision-making.

Research Philosophy

My research philosophy is based on the premise that cybersecurity problems are increasingly dynamic and cannot be addressed effectively through isolated signatures, static rules, or single-purpose security mechanisms. Modern security systems need to combine **behavioral intelligence, machine learning, risk assessment, automation, and secure system architecture**.

I therefore follow a research process that begins with identifying a practical security problem through systematic literature analysis, followed by architecture and model design, implementation, experimentation, comparative evaluation, and consideration of practical deployment.

A key feature of my research is the emphasis on **open-source and reproducible architectures**. I aim to develop research outcomes that can progress beyond theoretical models toward working prototypes and practical security solutions.

Current Research Focus

A major component of my research focuses on AI-based malware analysis and detection. Traditional malware detection approaches frequently depend on static signatures or predefined rules, which can become ineffective against rapidly evolving and obfuscated malware. My research therefore investigates the integration of machine learning and behavioral techniques with open-source architectures to improve malware analysis and threat identification.

One of my significant research contributions is MAOMLB: Advancing Malware Analysis with AI-Based Open-Source Architecture Integrating Machine Learning and Behavioral Techniques, published in the Journal of Applied Research and Technology. My related work includes BAOSAML, a Behavioral AI-Based Open-Source Architecture for Malware Analysis Using Machine Learning. These studies represent my effort to move beyond isolated machine-learning models toward integrated architectures capable of supporting practical cybersecurity analysis.

My research also explores deep learning, recurrent neural networks, attention mechanisms, risk prediction, and intelligent security orchestration. For example, my work on RNN-based rapid threat detection and response investigates machine learning approaches for reducing the time required to identify and respond to security threats. My conference research has additionally examined hierarchical attention mechanisms for risk prediction and AI-based Security Orchestration, Automation and Response systems.

Research Methodology and Technical Approach

My research methodology emphasizes a combination of problem formulation, systematic literature analysis, dataset-driven experimentation, machine learning/deep learning model development, comparative evaluation, and practical system implementation.

I am particularly interested in research problems where theoretical models can be translated into working prototypes. Depending on the problem, I explore techniques including machine learning, deep learning, recurrent neural networks, graph-based representations, attention mechanisms, behavioral analysis, risk modelling, and intelligent automation.

An important aspect of my research is the use of open-source technologies and reproducible architectures. I believe that cybersecurity research should not remain limited to theoretical evaluation or isolated benchmark experiments. Wherever possible, research outcomes should be capable of being implemented, evaluated, and integrated into realistic computing environments.

This philosophy has also influenced my work in DevOps and cloud-based security. My technical work includes CI/CD automation, cloud deployment, containerization, application security, and secure software development practices. I have developed hands-on learning and deployment resources involving GitHub, AWS CodeBuild, AWS CodePipeline, Amazon S3, Docker, and cloud-hosted applications.

Research Contributions

My research activities have resulted in publications across Scopus-indexed journals and international conferences, including Springer and IEEE venues. My academic work includes research in malware analysis, threat detection, risk prediction, security orchestration, virtual cybersecurity laboratories, generative AI applications, automated academic project management, smart examination systems, IoT, cloud computing, and AI-enabled applications.

I have also contributed to technology transfer through intellectual property. My patent portfolio includes work on risk-level analysis for AI-based open-source architecture and secure communication based on machine learning using IoT equipment.

Beyond publications, I consider student research mentorship an important part of my research contribution. I have guided projects involving AI-enabled asset management, financial risk assessment, academic project management using genetic algorithms and machine learning, virtual cybersecurity laboratories, generative AI-based educational frameworks, AI-based security orchestration, intelligent examination systems, IoT-enabled systems, and other applied computing problems.

Future Research Directions

My future research agenda will focus on four interconnected directions.

First, AI-driven adaptive cybersecurity. I intend to investigate explainable and adaptive AI techniques for malware detection, threat intelligence, risk prediction, and automated security response. A key objective will be to develop models that are not only accurate but also interpretable and useful for security analysts.

Second, graph-based and behavioral threat intelligence. Modern cyber threats involve complex relationships among users, processes, files, network entities, indicators of compromise, and attack stages. I aim to explore graph-based learning and dynamic representations for modelling these relationships and identifying emerging attack patterns.

Third, secure AI and open-source architectures. As AI-enabled applications increasingly depend on open-source components, libraries, models, APIs, and distributed services, systematic assessment of their security and risk becomes increasingly important. My future work will investigate frameworks for identifying, quantifying, and mitigating security risks in AI-based open-source ecosystems.

Fourth, DevSecOps and intelligent cloud security. I plan to explore the integration of AI-based security analysis into CI/CD pipelines and cloud-native environments. This includes automated vulnerability assessment, security policy enforcement, anomaly detection, secrets management, and intelligent security orchestration across containerized and cloud-based applications.

Ultimately, my goal is to establish a research program that connects AI, cybersecurity, cloud computing, and open-source technologies to address practical security problems. I aim to build collaborative research networks involving academic researchers, students, industry professionals, and open-source communities, while producing research that is scientifically rigorous, reproducible, and practically deployable.

Research Vision

My long-term research vision is to contribute toward the development of intelligent, explainable, adaptive, and secure computing systems capable of responding to continuously evolving cyber threats. I believe that the future of cybersecurity research lies not in a single detection algorithm or isolated security tool, but in the integration of AI, behavioral intelligence, automation, and secure system architecture.

Through interdisciplinary collaboration and student-centered research mentorship, I intend to develop a research environment where students can progress from identifying real-world problems to conducting systematic research, developing prototypes, evaluating results, and communicating their findings through high-quality scholarly publications and intellectual property.

My broader objective is therefore to bridge the gap between research innovation and real-world cybersecurity practice, contributing both academically and technologically to the development of secure intelligent computing systems.