MORIASI KEVIN MING'ATE

Location: Nairobi, Kenya

Email: emkevin254@gmail.com

LinkedIn: linkedin.com/in/kevin-moriasi-5a662625b

GitHub: https://github.com/cyb3r-cych0

PROFESSIONAL SUMMARY

Detail-oriented and driven Computer Science Graduate with a Master of Science, specializing in the intersection of Artificial Intelligence, Machine Learning, and Cybersecurity. Proven track record in empirical academic research with first-author publications in IEEE and Springer, along with active ongoing research in self-supervised IoT anomaly detection. Complemented by hands-on technical experience in full-lifecycle web application penetration testing using Kali Linux, Nmap, Burp Suite, and SQLmap during a professional tenure at Mindenious Edutech LLP. Highly proficient in engineering Python-based AI defenses, training large-scale predictive ensemble architectures on multi-decade data arrays, and simulating complex threat scenarios to evaluate system resilience. Eager to leverage this comprehensive toolkit in Cybersecurity, Large Language Models (LLMs), and secure systems building in the technology industry.

EDUCATION

Master of Science in Computer Science

Karpagam Academy of Higher Education – Coimbatore, Tamil Nadu, India | July 2026

- **GPA / Honors:** 8.63 / 10.0 | First Class with Distinction
- **Specialization:** Cybersecurity and Artificial Intelligence / Machine Learning (AI/ML)
- **Relevant Coursework:** Cybersecurity Fundamentals, Advanced Machine Learning, Applied Cryptography, Web Application Security, Data Protection & Privacy, Cloud Security, Neural Networks.

Bachelor of Business Information Technology

Kenya Methodist University – Nairobi, Kenya | October 2023

- **GPA / Honors:** 3.34 / 4.0 | Second Class Honors (Upper Division)

PUBLICATIONS & RESEARCH IN PROGRESS

1. **Ming'ate M., Yuvaraj K.** (2025). "AI-based XSS Vulnerability Scanner with Context-Aware Remediation for Web Application Security." Published in IEEE Proceedings of the 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA).

2. **Irankunda E., Ming'ate K.** (2026). "Statistical and Machine Learning Modeling of Long-Term PM2.5 Variability Across East, Central, and Southern Africa." Published in Springer Water, Air, & Soil Pollution, 237, 826.

3. **Ming'ate K., Irankunda E.** (2026). "Self-Supervised Representation Learning for Explainable Detection of Tampered Air Pollution Sensor Data." In Preparation targeting peer-reviewed publication.

RESEARCH EXPERIENCE

Graduate Researcher (Generative AI & Web Security)

Karpagam Academy of Higher Education | October 2025 – Present

- Developed VulScanWare, an autonomous, Python-based AI vulnerability framework engineered to mitigate client-side Cross-Site Scripting (XSS) anomalies.
- Designed a multi-stage software pipeline integrating target-directed web crawling, algorithmic threat identification, and a Large Language Model (LLM) agent.
- Benchmarked the framework against industry standards (Burp Suite, Acunetix) utilizing vulnerable sandboxes (DVWA and Mutillidae).
- Achieved high detection accuracy and precision, effectively minimizing false-positive and false-negative alert rates.
- Slashed remediation response latency by embedding context-aware auto-patching rules directly via the LLM pipeline.

Data Science Researcher (Large-Scale Predictive Modeling)
Karpagam Academy of Higher Education | April 2026 – Present

- Engineered a scalable data science pipeline to ingest and process 25 years (2000–2025) of continuous MERRA-2 meteorological and time-series arrays.
- Trained, hyper-tuned, and compared predictive Ensemble ML models (Gradient Boosting, Random Forest) alongside regularized regressions (Lasso, Ridge).
- Attained excellent predictive performance with Ensemble models, yielding a strong R^2 and slope metric.
- Executed standardized multi-variable regression analysis to isolate and mathematically prove that thermal dynamics heavily dictate data shifts over wind vectors in data-scarce domains.

Lead Researcher (IoT Security & Cyber-Physical Anomaly Detection)
Karpagam Academy of Higher Education | Active Project

- Developed an environmental cybersecurity evaluation framework to secure IoT-based sensing infrastructure against malicious data tampering.
- Modeled four representative sensor data integrity attack scenarios: Constant Bias Injection, Gradual Drift, Spike Suppression, and Random Stealth Perturbation using real-world OpenAQ data.
- Programmed and benchmarked three distinct anomaly detectors: a Rolling Z-score statistical filter, a Reconstruction Error neural model, and an Isolation Forest model.
- Evaluated adversarial resilience using multi-metric validation metrics including Accuracy, Precision, Recall, F1-Score, and False Positive Rates (FPR).

PROFESSIONAL EXPERIENCE

Cybersecurity Research Intern | Mindenious Edutech LLP – Bangalore, Karnataka, India
January 2026 – February 2026

- Executed a full-lifecycle, end-to-end web application penetration testing regime utilizing Kali Linux against target images on Metasploitable2.
- Managed the complete penetration testing lifecycle spanning active reconnaissance, weaponized exploitation, and post-exploit impact reporting.
- Deployed Nmap for network topology mapping and targeted port discovery; utilized Burp Suite for HTTP parameter tampering, session hijacking, and authentication bypass assessments.
- Conducted structured vulnerability scanning using SQLmap to intercept, parse, and exploit backend database interaction flaws.
- Authored thorough technical vulnerability disclosures detailing exact step-by-step remediation procedures to enforce strict client-side data protection.

TECHNICAL SKILLS

- **Core Programming & Scripting:** Python (Advanced Data Structures, Object-Oriented), SQL, Shell Scripting (Bash).
- **AI/ML and Neural Frameworks:** Scikit-Learn, TensorFlow, PyTorch, Hugging Face Transformers, Gradient Boosting (XGBoost, LightGBM), Random Forest, Regularized Regressions (Lasso, Ridge), Isolation Forests.
- **Offensive Cybersecurity and Pentesting:** Kali Linux, Nmap, Burp Suite (Professional/Community), SQLmap, Metasploit Framework, Wireshark, Web Vulnerability Environments (DVWA, Mutillidae, Metasploitable2).
- **Defensive Engineering and Protocols:** Cryptographic Implementation (AES, RSA, SHA-256), Input Validation, Context-Aware Auto-Remediation, Vulnerability Lifecycle Management, Data Protection Controls.

- **Data Engineering and Environments:** Git/GitHub Version Control, Linux/Unix System Administration, Jupyter Architecture, Pandas, NumPy, Large-scale Multi-Dimensional Dataset Management (MERRA-2, OpenAQ API).

REFERENCES

1. **Dr. S. Mythili** – MCA, M.Phil, Ph.D, SET, NET, Professor and Head, Computer Science Department, Faculty of Arts, Science, Commerce and Management, Karpagam Academy of Higer Education Pollachi Main Road, Eachanari Post, Coimbatore - 641 021, Tamil Nadu, India., cs.hod@kahedu.edu.in
2. **Dr. Elisephane Irankunda.** – Mubadala Arabian Center for Climate and Environmental Sciences (Mubadala ACCESS), New York University Abu Dhabi, Saadiyat Marina District, PO Box 129188, Abu Dhabi, United Arab Emirates, elisephane@gmail.com.
3. **POOJAVAANI** – Mindenious Edutech LLP, Cybersecurity Internship, 5, 14th Main Road, 15th Cross Rd, Sector 4, HSR Layout, Bengaluru, Karnataka 560102, pooja@mindenious.in