Yuning **JIANG**

SG-PR | yuning-j | Yuning-J | (+65)80382055 | yuning.jiang17@gmail.com | Personal Website | Publications

Experience

OCT.2023 – Present | **Research Fellow** , NUS-NCS Joint Cybersecurity Lab, National University of Singapore, Singapore

Developed a **dual-graph vulnerability management** framework integrating CVSS/EPSS to improve **patch prioritization** in IT and ICS environments. The approach supports NIST SP 800-160-aligned practices and enhances **decision explainability** for security teams.

- Designed asset-risk graph models and ranking algorithms for vulnerability mitigation.
- Evaluated performance on real-world enterprise and ICS datasets.

Built a simulation platform for attacker-defender interactions using MITRE ATT&CK and **LLM-based threat intelligence**. Supports **proactive patch planning** under dynamic and incomplete information.

- Architected Python-based collectors and processors (with Dockerized Neo4j) to ingest and normalize CVE, CPE, ExploitDB, CISA, etc., capturing over 300K vulnerability nodes and multi-relation edges.
- Developed a RAG module that fuses graph lookups with LLM prompts.
- Wrote advanced queries for multi-hop exploit path discovery and business-impact scoring to drive a POMDP-style attacker decision engine.
- Engineered a scheduling algorithm that ingests live threat intelligence and graph projections to prioritize remediation actions under budget constraints.

Collaborated with NCS Pte Ltd to design and implement algorithms for advanced incident analysis.

- Reduced alert volume by over 74%.
- Enhanced NIDS precision by aligning network alerts with MITRE ATT&CK, achieved 89% and 83.8% precision for tactic and technique classification, respectively.

OCT.2022 – OCT.2023 | **Research Fellow** , NTU-WeBank Lab, Nanyang Technological University, Singapore

Developed a knowledge graph tool for WeBank to enable **automated test case construction**.

- Led end-to-end development : system design, model training, coding, and deployment in WeBank.
- Optimized NER performance and downstream workflow efficiency through task-specific fine-tuning.

AUG.2017 – SEP.2022 | **PhD Candidate** , University of Skövde, Sweden

Developed AI-based tools to automate **vulnerability retrieval** and risk scoring. The work aimed to improve intelligence extraction and prioritize mitigation based on system-specific configurations.

- Designed an Ansible-based tool for automated configuration extraction from Windows/Linux systems.
- Developed RoBERTa-based NER (98.6%) and RE (97.4%) models for extracting vulnerability mentions ; achieved 76.6% precision and 92.6% coverage in **end-to-end retrieval**.
- Built an ensemble ML pipeline for **scoring vulnerabilities using multiple contextual features**.

Developed system models for enterprise and ICS environments to support **secure-by-design** analysis and compliance validation. The models were aligned with IEC 62351 and NIST SP 800-82 standards.

- Modeled power grid configurations and **system dependencies** for security validation.
- Ensured compliant integration of ICS system specifications into the cybersecurity modeling pipeline.
- Facilitated simulation-based training for ICS operators to improve incident response readiness.
- Conducted case studies with local power grid companies.

Teaching and course leadership :

- Master Course *Cybersecurity for IoT and Critical Infrastructures* (Co-Leader).
- Master Course *Information and Cyber Security : Principles and Practices* (Leader).
- Undergraduate Courses *Object-Oriented Programming* and *Algorithm and Data Structure* (Co-Leader).

Jan.2015 – Sep.2015 | **Research Projects** , King's College London, United Kingdom

Contributed to a smart city research project that analyzed traffic patterns to predict transportation preferences under varying urban conditions.

AUG.2016 – JUN.2017 | **Data Product Manager** , Beijing Changjiu Logistics Co., Ltd., China

Led data product development for financial risk prediction in automotive dealership loans, improving operational insight across over 6,600 dealerships and 100+ car brands.

- Built predictive models for financial risk assessment, 85% accuracy in identifying high-risk dealers.
- Led a cross-functional team of 10 to design, develop, and deploy data-driven decision tools.
- Integrated statistical modeling, data visualization, and relational databases into a scalable pipeline.

Education

AUG.2017 – SEP.2022 | **PhD in Informatics, University of Skövde, Sweden**
Thesis Topic : *Cyber Vulnerability Analysis for Critical Infrastructures*.

SEPT.2014 – JAN.2016 | **MSc in Electronic Engineering with Business Management, King's College London, United Kingdom**
Thesis Topic : *Case Study of Internet Access in Developing Countries*.

SEPT.2010 – JUN.2014 | **BSc (Eng) in Electronics and Information, Beihang University, China**
Thesis Topic : *Optimal Energy Management Strategy of Fuel Cell Hybrid Power Systems*.

Honors and Awards

- 2022 Länsförsäkringar Skaraborg Prize, issued by Skaraborgs Academy on Outstanding PhD Thesis
- 2021 Prize for AI, Art and Society in "SAAI Factory - Hackathon on Art and AI", issued by Super Artistic AI FACTORY
- 2021 Anthony Parker Memorial Prize, issued by R. U. Hacking? (Reading University Hacking)
- 2019 Young CRITIS Award, issued by the 14th International Conference on Critical Information Infrastructure Security

Funding and Scholarship

- 2022 Vinnova funding (113,000 SEK) on applied research validation
- 2019 IPSI (Industrial PhD School in Informatics) Scholarship
- 2017 European Union - Internal Security Fund
- 2014 BeiHang University YuanHang Global Study Scholarship

Skills

Programming	Python, Java, C
Tools	Fortinet SIEM/SOAR, Rapid7 InsightVM, Tenable, Claroty, Suricada
Methodologies	Risk Analysis, MITRE ATT&CK, Zero-Trust Architecture, Model-Based Security Engineering
Database	MongoDB, MySQL, Neo4j, Apache Spark
ML/NLP	TensorFlow, PyTorch, Hugging Face Transformers

Publications within Last 5 Years

- 2025 **Jiang, Y.**, Wang, H., Meng, Q., Oo, N., Lim, H., & Sikdar, B. (2025). *VulCPE : Context-Aware Cybersecurity Vulnerability Retrieval and Management* (under review) arXiv : [2505.13895]
- 2025 **Jiang, Y.**, Oo, N., Meng, Q., Sikdar, B., & Lim, H. (2025). *VulRG : Multi-Level Explainable Vulnerability Patch Ranking for Complex Systems Using Graphs* (under review) arXiv : [2502.11143]
- 2025 **Jiang, Y.**, Oo, N., Meng, Q., Sikdar, B., & Lim, H. (2025). *MITRE ATT&CK Application in Threat Intelligence and The Way Forward* (under review) arXiv : [2502.10825]
- 2024 **Jiang, Y.**, Oo, N., Meng, Q., Sikdar, B., & Lim, H. (2024). *A Survey on Vulnerability Prioritization : Taxonomy, Metrics, and Research Challenge* (under review) arXiv : [2502.11070]
- 2024 Meng, Q., Oo, N., **Jiang, Y.**, Lim, H. W., & Sikdar, B. (2024). *M2ASK : A Correlation-Based Multi-Step Attack Scenario Detection Framework Using MITRE ATT&CK Mapping.* In : Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (pp. 4979-4981). (Poster Link)
- 2024 **Jiang, Y.**, Jeusfeld, M., Mosaad, M., & Oo, N. (2024). *Enterprise architecture modeling for cybersecurity analysis in critical infrastructures-A systematic literature review.* In : International Journal of Critical Infrastructure Protection, 100700. (Paper Link)
- 2024 **Jiang, Y.**, Wang, W., Ding, J., Lu, X., & Jing, Y. (2024). *Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber–Physical Production Systems.* In : Future Internet 2024, 16, 134. (Paper Link)
- 2023 **Jiang, Y.**, Li, R., Xing, Z., & Zhao, X. (2023). *A Method for Software Test Case Recommendation based on Knowledge Graph* (Patent Link)
- 2023 **Jiang, Y.**, Jeusfeld, M., Ding, J., & Sandahl, E. (2023). *Model-Based Cybersecurity Analysis : Extending Enterprise Modeling to Critical Infrastructure Cybersecurity* In : Business & Information Systems Engineering, 1-34. (Paper Link)
- 2022 **Jiang, Y.** (2022). *Vulnerability Analysis for Critical Infrastructures.* (Thesis Link)
- 2022 **Jiang, Y.**, & Atif, Y. (2022). *Towards automatic discovery and assessment of vulnerability severity in cyber-physical systems.*. Array, p.100209. (Paper Link)
- 2021 **Jiang, Y.**, & Atif, Y. (2021). *A Selective Ensemble Model for Cognitive Cybersecurity Analysis*. Journal of Network and Computer Applications, 193, 103210. (Paper Link)
- 2021 **Jiang, Y.**, Jeusfeld, M., & Ding, J. (2021, August). *Evaluating the Data Inconsistency of Open-Source Vulnerability Repositories*. In 4th International Workshop on Cyber Threat Intelligence Management (CyberTIM 2021) of 16th International Conference on Availability, Reliability and Security (ARES 2021). (Paper Link)