# Bishnu Bhusal

✉ bhusalb@missouri.edu
bishnubhusal.com.np
bhusalb

## Education

2022–Present **Ph.D. in Computer Science**, *University of Missouri*, Columbia MO, USA.
*GPA: 4.0 / 4.0*
Advisor: Rohit Chadha
Thesis: Automated Verification of Differentially Private Algorithms
Expected graduation in **May 2026**

2022–2024 **M.S. in Computer Science**, *University of Missouri*, Columbia MO, USA.
Along with a minor in Statistics and a Graduate Certificate in Cybersecurity
*GPA: 4.0 / 4.0*
Project: Formal verification for blockchain-based insurance claims processing

2013–2017 **B.Eng. in Computer Engineering**, *Tribhuvan University*, Kathmandu, Nepal.

## Research Interests

Cybersecurity, Privacy, Machine Learning and Formal Methods

## Research Experience

2022–Present **Graduate Research Assistant**, *University of Missouri*, Columbia.

- Contributed to two NSF grant proposals on differential privacy verification and quantum machine learning education, writing technical sections, preliminary results, and research project designs (PI: Rohit Chadha, under review)
- Designed and implemented approximate algorithms to verify differential privacy with Gaussian noise, proving the almost decidability of ($\varepsilon$, $\delta$)-DP.
- Developed PSPACE-complete algorithms for verifying differential privacy of online randomized algorithms using DiP automata with multiple real-valued variables, and implemented the verification tool.
- Extended $\delta$-decision procedures to handle integrals over real functions.
- Developed a risk-adaptive secure communication system for drones in warfare scenarios within the Arculus framework, integrating certificate-based and symmetric key encryption to ensure mission resilience. Adopted by the U.S. Marines for training exercises.
- Performed formal verification of blockchain smart contracts, enhancing reliability and efficiency in insurance claim processing.
- Developed a game-theoretic ransomware defense model using deception strategies, demonstrating effectiveness in protecting critical infrastructures.

Summer 2025 **Summer Fellow**, *Quantum Innovation Center at Mizzou*, Columbia, MO.

- Researched differentially private quantum machine learning, demonstrating that quantum noise strengthens privacy and establishing theoretical guarantees for hybrid quantum–classical models.

Fall 2024 **Research Intern**, *SRI International*, Menlo Park, CA.

- Designed and implemented a novel privacy-preserving in-context learning framework for LLMs, outperforming state-of-the-art methods on most benchmarks.

Summer 2024 **Applied Scientist Intern**, *Amazon*, Santa Clara, CA.

- Developed techniques to prevent copyright violations in LLM responses within retrieval-augmented generation systems

## Teaching Experience

2023–Present **Graduate Teaching Assistant**, *University of Missouri*, Columbia.

- Assist in CS 7420: Software Security; redesigned SEED lab exercises and course modules, graded student submissions, and developed a module on prompt injection attacks in LLMs to illustrate modern security challenges.
- Conduct weekly labs for CS 1050: Algorithm Design and Programming I, mentoring students in C programming and managing lab grading.
- Grade assignments and hold office hours for CS 4320: Software Engineering I, CS 8450: Formal Engineering Methods for Software and Security, CS 8460: Cryptographic Protocols and Formal Proofs, and Special Course: Introduction to Quantum Computing.

2019–2021 **Adjunct Lecturer**, *Orchid International College*, Kathmandu, Nepal.

- Designed and taught courses on cryptography, software design and analysis, and machine learning.
- Led hands-on laboratory sessions on implementing both symmetric and asymmetric encryption algorithms.

## Publications

AAAI'26 **Bhusal, B.**, Acharya, M., Kaur, R., Samplawski, C., Roy, A., Cobb, A.D., Chadha, R., and Jha, S.: Privacy Preserving In-Context-Learning Framework for Large Language Models. In Proceedings of the 40th AAAI Conference on Artificial Intelligence (AAAI-26), 2026. CORE ranking: **A***

CCS'25 **Bhusal, B.**, Chadha, R., Sistla, A. P., and, Viswanathan, M. Approximate Algorithms for Verifying Differential Privacy with Gaussian Distributions. Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. CORE ranking: **A***

CCS'23 Chadha, R., Sistla, A. P., Viswanathan, M., and **Bhusal, B.**. Deciding differential privacy of online algorithms with multiple variables. Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. CORE ranking: **A***

OOPSLA'25 Rivera C.,**Bhusal, B.**, Chadha, R., Sistla, A. P., and, Viswanathan, M. . Checking $\delta$-Satisfiability of Reals with Integrals. Proceedings of the ACM on Programming Languages 9.OOPSLA1 (2025). CORE ranking: **A**

HCII'25 **Bhusal, B.**, Ma, Y, Chadha, R. Privacy Nutrition Labels: Promise, Practice, and Paradoxes in Communicating Privacy. In International Conference on Human-Computer Interaction Posters (pp. 18–28). Springer.

GameSec'24 🏆 Neupane, R. L., **Bhusal, B.**, Neupane, K., Regmi, P., Dinh, T., Marrero, L., Saghaian N. E., S. M., Nadendla, V. S. S., and Calyam, P. On countering ransomware attacks using strategic deception. In Proceedings of the Conference on Decision and Game Theory for Security (GameSec). 2024. **Best Paper Award Winner.**

NOMS'24 Neupane Lal R., Bonnah E., **Bhusal, B.**, Neupane K., Hoque Anuarul K, Calyam P. Formal Verification for Blockchain-based Insurance Claims Processing. In Proceedings of the NOMS 2024 - 37th IEEE/IFIP Network Operations and Management Symposium

SIGCITE'25 Chapagain, D., **Bhusal, B.**, Kshetri, N., & Subedi, P. RealPhish: An Algorithm for Real-Time Email Phishing Detection. In Proceedings of the 26th Annual Conference on Information Technology Education. 2025.

### Book Chapters

CRC Press Osama, O. F., **Bhusal, B.**, Kshetri, N., and Pokharel, B. P. blockDADS: Blockchain Technology for Data Analytics and Data Security - Applications and Solutions. In Blockchain Technology for Cyber Defense, Cyber Security, and Countermeasures: Techniques, Solutions, and Applications. CRC Press, Routledge Taylor & Francis Group, 2024.

IGI Global Rahman, M. M., Hossain, S., **Bhusal, B.**, & Kshetri, N. (2025). cyberAItrends: Future trends in AI for cyberbullying prevention. In K. K. Reddy C., M. Malhotra, M. Ouaissa, M. M. Hanafiah, & M. Shuaib (Eds.), Combating cyberbullying with generative AI. IGI Global.

### Drafts and Preprints

Secure Insurance Claims Processing using Formal Modeling and Reliable Threat Mitigation. Submitted to Journal

UAVchain: A Study of Blockchain Technology Applications for Unmanned Aerial Vehicles: Safety, Security, Directions, and Challenges. Submitted to Journal

arxiv Adhikari, S., Bhusal B., Ghimire, P., and Shrestha, A. Vton-it: Virtual try-on using image translation.

## Academic Service

**Program Committee Member**, *AAAI'26, PPAI'25*.

**Artifact Evaluation Committee Member**, *PETS'26, PETS'25, CAV'25, CCS'23*.

**Journal Reviewer**, *IEEE Access*.

**Student Volunteer**, *AAAI'26*.

## Awards

2026 **AAAI'26 Student Travel Scholarship**.

2025 **Quantum Innovation Center Summer Fellowship $7,500**.

2025 **ACM CCS 2025 Student Travel Grant**.

2025 **EECS Excellence Travel Grant**, *University of Missouri*, Columbia.

2024 **GameSec 2024 Best Paper Award**.

2024 **IEEE CSF Travel Grant**.

2024 **Winner**, *GPC Interdisciplinary Case Competition*, University of Missouri, Columbia.

2023 **EECS Excellence Travel Grant**, *University of Missouri*, Columbia.

2023 **IEEE SaTML Travel Grant**, *IEEE SaTML*.

2022 **EECS Excellence Fellowship**, *University of Missouri*, Columbia.

2015 **Runner-up**, *KEC LITE Software Competition*, Kathmandu, Nepal.

## Talks

2025 **Automated Verification of Differentially Private Algorithms**, *Invited Talk, The National Institute of Advanced Industrial Science and Technology*, Tokyo, Japan.

2025 **Approximate algorithms for verifying differential privacy with gaussian distributions**, *Conference Presentation, CCS'25*, Taipei, Taiwan.

2025 **Checking $\delta$-Satisfiability of Reals with Integrals**, *Conference Presentation, OOPSLA'25*, Singapore.

2025 **Advancing Differentially Private Quantum Machine Learning**, *Invited Talk, Quantum Day, University of Missouri*, Columbia, MO, USA.

2023 **Deciding Differential Privacy of Online Algorithms with Multiple Variables**, *Conference Presentation, CCS'23*, Copenhagen, Denmark.

## Industry Experience

2020–2022 **Software Engineer**, *Geoedge*, New York, USA (Remote).

- Designed and scaled microservices handling 1.5B daily requests and petabytes of Elasticsearch data.
- Migrated services to Kubernetes with custom auto-scaling metrics, improving uptime and reducing cloud costs by 35%.
- Enhanced CI/CD processes, cutting downtime by 25% for business-critical operations.

2020–2020 **Software Engineer**, *Furitech*, Tel Aviv, Israel (Remote).

- Led full-stack development of a venture capital information management system using Django and Angular.
- Contributed to software lifecycle from requirements to deployment, consistently achieving high customer satisfaction.

2018–2020 **Software Engineer**, *Hashunited*, Tel Aviv, Israel (Remote).

- Built microservice-based platforms for cryptocurrency mining and auto-trading with near-zero downtime.
- Developed analytics dashboards (Grafana, InfluxDB) and predictive algorithms for cryptocurrency trends.

2017–2018 **Software Engineer**, *Sustainable Technological Solutions*, Kathmandu, Nepal.

- Developed an Exam Management System (Java, Spring Boot, Vue.js, Postgres) serving 1M students and adopted by 20+ government bodies.

## Workshops and Summer Schools

2023 **Formal Techniques**, *SRI*, Atherton, CA.

## Leadership and Volunteering Activities

2024 **President**, *EECS Graduate Student Association*, University of Missouri, Columbia.

2023 **Secretary**, *EECS Graduate Student Association*, University of Missouri, Columbia.

## Certifications

2023 **AWS Associate Solutions Architect (SAA-C03)**, *by AWS*.

2023 **Graduate Certificate in Cybersecurity**, *by University of Missouri*, Columbia.

2020 **Deep Learning Specialization**, *by deeplearning.ai*.

## Software

DiPApprox DiPApprox is a tool for verifying differential privacy of DiPGauss programs, providing automated checks, counterexamples, and including all benchmark examples and evaluation scripts. `https://github.com/bhusalb/approximate-dp`.

$\int$Dreal A $\delta$-decision procedure for quantifier-free and $\exists^*\forall^*$ fragments of first-order logic over the Reals, built on top of `dReal4`. Also contains a benchmark suite of 41 queries and evaluation scripts. `https://github.com/codyjrivera/int-dreal-artifact`

DiPAut DiPAut is a Python tool for verifying the differential privacy of automata. It analyzes a given DiPA, determines if it is well-formed, computes a privacy weight when applicable, and identifies potential privacy violations. The tool also includes a full suite of benchmark examples and evaluation scripts. `https://github.com/bhusalb/DiPAut`

## References

Rohit Chadha
Associate Professor and Director of Cybersecurity Center
EECS, University of Missouri, Columbia
Email: chadhar@missouri.edu

Mahesh Viswanathan
Professor
Department of Computer Science, University of Illinois at Urbana-Champaign
Email: vmahesh@illinois.edu

Aravinda Prasad Sistla
Professor
Department of Computer Science, University of Illinois at Chicago
Email: sistla@uic.edu

Prasad Calyam
Professor and Director of the Center for Cyber Education, Research and Infrastructure
EECS, University of Missouri, Columbia
Email: calyamp@missouri.edu