Bimal Viswanath

Assistant Professor

Virginia Tech
Department of Computer Science
✉ *vbimal@cs.vt.edu*
🖱 *people.cs.vt.edu/vbimal*

Research interests

Security and machine learning; Data-driven security and privacy; Measurement and analysis of networked systems

Education

2008–2016 **Ph.D. in Computer Science** (*Summa cum laude*)
Saarland University and Max Planck Institute for Software Systems (MPI-SWS), Kaiserslautern/Saarbruecken, Germany
Advisors: Prof. Krishna P. Gummadi, Prof. Alan Mislove

2005–2008 **Master of Science in Computer Science and Engineering**
Indian Institute of Technology Madras, Chennai, India
Advisor: Prof. C. Siva Ram Murthy

2001–2005 **Bachelor of Technology in Computer Science and Engineering**
Cochin University of Science and Technology, Cochin, India

Employment History

2018–Present **Assistant Professor (tenure-track)**
Department of Computer Science, Virginia Tech, Blacksburg, VA, USA

2017–2018 **External Postdoctoral Researcher**
Department of Computer Science, University of Chicago, Chicago, IL, USA
Research topic: Systems and Network Security

2016–2018 **Postdoctoral Scholar**
Department of Computer Science, University of California, Santa Barbara, CA, USA
Research topic: Systems and Network Security

2015–2016 **Researcher**
Nokia Bell Labs, Stuttgart, Germany
Research topic: Cloud Computing, Data Analytics

2008–2015 **Ph.D. Candidate**
Max Planck Institute for Software Systems, Kaiserslautern/Saarbruecken, Germany
Research topic: Security and Privacy in Social Computing Systems

2005-2008 **Graduate Student**
Department of Computer Science and Engineering, Indian Institute of Technology Madras, Chennai, India
Research topic: Optical Burst Switching Networks

Honors and Awards

2020 AI2000 Most Influential Scholar Award Honorable Mention for being among the top 100 most cited scholars in computer networking from 2009-2019 (Source: `https://www.aminer.org/ai2000/cn`)

2015 Best Paper Award, ACM Conference on Online Social Networks (COSN)

2014 Distinguished Paper Award, Symposium on Usable Privacy and Security (SOUPS)

Publications

Total Citations: 7181, H-Index: 25 (Source: Google Scholar as of July 2024)

IEEE S&P'24 **An Analysis of Recent Advances in Deepfake Image Detection in an Evolving Threat Landscape**
Sifat Muhammad Abdullah, Aravind Cheruvu, Shravya Kanchi, Taejoong Chung, Peng Gao, Murtuza Jadliwala, and Bimal Viswanath.
IEEE S&P'24, San Francisco, CA, May 2024.

ACSAC'23 **A First Look at Toxicity Injection Attacks on Open-domain Chatbots**
Connor Weeks (co-lead), Aravind Cheruvu (co-lead), Sifat Muhammad Abdullah, Shravya Kanchi, Daphne Yao, and Bimal Viswanath.
ACSAC'23, Austin, TX, December 2023.

ACM TSEM **Measurement of Embedding Choices on Cryptographic API Completion Tasks**
Ya Xiao, Wenjia Song, Salman Ahmed, Xinyang Ge, Bimal Viswanath, Na Meng, and Danfeng (Daphne) Yao.
ACM Transactions on Software Engineering and Methodology, 2023.

IEEE TSE **Specializing Neural Networks for Cryptographic Code Completion Applications**
Ya Xiao, Wenjia Song, Jingyuan Qi, Bimal Viswanath, Patrick McDaniel, Danfeng (Daphne) Yao.
IEEE Transactions on Software Engineering, 2023.

IEEE S&P'23 **Deepfake Text Detection: Limitations and Opportunities**
Jiameng Pu, Zain Sarwar, Sifat Muhammad Abdullah, Abdullah Rehman, Yoonjin Kim, Parantapa Bhattacharya, Mobin Javed and Bimal Viswanath.
IEEE S&P'23, San Francisco, CA, May 2023.

USENIX Security'21 **T-Miner: A Generative Approach to Defend Against Trojan Attacks on Deep Text Models**
Ahmadreza Azizi, Ibrahim Asadullah Tahmid, Asim Waheed, Neal Mangaokar, Jiameng Pu, Mobin Javed, Chandan K. Reddy and Bimal Viswanath.
USENIX Security, Online, August 2021.

WWW'21 **Deepfake Videos in the Wild: Analysis and Detection**
Jiameng Pu, Neal Mangaokar, Lauren Kelly, Parantapa Bhattacharya, Kavya Sundaram, Mobin Javed, Bolun Wang, and Bimal Viswanath.
WWW, Online, April 2021.

ACSAC'20 **NoiseScope: Detecting Deepfake Images in a Blind Setting**
Jiameng Pu, Neal Mangaokar, Bolun Wang, Chandan K. Reddy, and Bimal Viswanath.
ACSAC, Online, December 2020

IEEE EuroS&P'20 **Jekyll: Attacking Medical Image Diagnostics using Neural Translation**
Neal Mangaokar, Jiameng Pu, Parantapa Bhattacharya, Chandan K. Reddy, and Bimal Viswanath.
IEEE EuroS&P, Online, September 2020

IEEE S&P'20 **Throwing Darts in the Dark? Detecting Bots with Limited Data using Neural Data Augmentation**
Steve T.K. Jan, Qingying Hao, Tianrui Hu, Jiameng Pu, Sonal Oswal, Gang Wang, and Bimal Viswanath.
IEEE S&P, Online, USA, May 2020

AsiaCCS'19 **What Happens After You Leak Your Password: Understanding Credential Sharing on Phishing Sites**
Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, and Gang Wang
AsiaCCS, Auckland, New Zealand, July 2019

IEEE S&P'19 **Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks**
Bolun Wang, Yuanshun Yao, Shawn Shan, Huiying Li, Bimal Viswanath, Haitao Zheng, and Ben Y. Zhao
IEEE S&P, San Francisco, CA, USA, May 2019

USENIX Security'18 **With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning**
Bolun Wang, Yuanshun Yao, Bimal Viswanath, Haitao Zheng, and Ben Y. Zhao
USENIX Security, Baltimore, MD, USA, August 2018

EuroS&P'18 **I Spy with My Little Eye: Analysis and Detection of Spying Browser Extensions**
Anupama Aggarwal, Bimal Viswanath, Liang Zhang, Saravana Kumar, Ayush Shah, and Ponnurangam Kumaraguru
EuroS&P, London, United Kingdom, April 2018

CoNEXT'17 **Towards Reliable Application Deployment in the Cloud**
Ruichuan Chen, Istemi Ekin Akkus, Bimal Viswanath, Ivica Rimac, and Volker Hilt
CoNEXT, Seoul, South Korea, December 2017

Middleware'17 **Sieve: Actionable Insights from Monitored Metrics in Distributed Systems**
Jörg Thalheim, Antonio Rodrigues, Istemi Ekin Akkus, Pramod Bhatotia, Ruichuan Chen, Bimal Viswanath, Lei Jiao, and Christof Fetzer
Middleware, Las Vegas, NV, USA, December 2017

IMC'17 **Complexity vs. Performance: Empirical Analysis of Machine Learning as a Service**
Yuanshun Yao, Zhujun Xiao, Bolun Wang, Bimal Viswanath, Haitao Zheng, and Ben Y. Zhao
IMC, London, UK, November 2017

CCS'17 **Automated Crowdturfing Attacks and Defenses in Online Review Systems**
Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, and Ben Y. Zhao
CCS, Dallas, TX, USA, October 2017

WWW'16 **Strengthening Weak Identities Through Inter-Domain Trust Transfer**
Giridhari Venkatadri, Oana Goga, Changtao Zhong, Bimal Viswanath, Krishna P. Gummadi, and Nishanth Sastry
WWW, Montreal, Canada, April 2016

COSN'15 **Strength in Numbers: Robust Tamper Detection in Crowd Computations**
Bimal Viswanath, M. Ahmad Bashir, M. Bilal Zafar, Simon Bouget, Saikat Guha, Krishna P. Gummadi, Aniket Kate, and Alan Mislove
COSN, Stanford University, CA, USA, November 2015

USENIX Security'14 **Towards Detecting Anomalous User Behavior in Online Social Networks**
Bimal Viswanath, Muhammad Ahmad Bashir, Mark Crovella, Saikat Guha, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove
USENIX Security, San Diego, CA, USA, August 2014

SOUPS'14 **Understanding and Specifying Social Access Control Lists**
Mainack Mondal, Yabing Liu, Bimal Viswanath, Krishna P. Gummadi, and Alan Mislove
SOUPS, Menlo Park, CA, USA, July 2014

CoNEXT'12 **Defending Against Large-scale Crawls in Online Social Networks**
Mainack Mondal, Bimal Viswanath, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove, and Ansley Post
CoNEXT, Nice, France, December 2012

WOSN'12 **Keeping Information Safe from Social Networking Apps**
Bimal Viswanath, Emre Kıcıman, and Stefan Saroiu
WOSN, Helsinki, Finland, August 2012

EuroSys'12 **Canal: Scaling Social Network-based Sybil Tolerance Schemes**
Bimal Viswanath, Mainack Mondal, Krishna P. Gummadi, Alan Mislove, and Ansley Post
EuroSys, Bern, Switzerland, April 2012

WWW'12 **Understanding and Combating Link Farming in the Twitter Social Network**
Saptarshi Ghosh (*co-primary author*), Bimal Viswanath (*co-primary author*), Farshad Kooti, Naveen Kumar Sharma, Korlam Gautam, Fabricio Benevenuto, Niloy Ganguly, and Krishna P. Gummadi
WWW, Lyon, France, April 2012

COMSNETS'12 **Exploring the Design Space of Social Network-based Sybil Defenses** *(Invited Paper)*
Bimal Viswanath, Mainack Mondal, Allen Clement, Peter Druschel, Krishna P. Gummadi, Alan Mislove, and Ansley Post
COMSNETS, Bangalore, India, January 2012

2011 **A Stochastic Model for the Behavior of Multiple TCP NewReno Sources over Optical Burst Switching Network**
Bimal Viswanath, T. Venkatesh, and C. Siva Ram Murthy
Photonic Network Communications, October 2011

NOSSDAV'11 **Sharing Social Content from Home: A Measurement-driven Feasibility Study**
Massimiliano Marcon, Bimal Viswanath, Meeyoung Cha, and Krishna P. Gummadi
NOSSDAV, Vancouver, Canada, June 2011

SIGCOMM'10 **An Analysis of Social Network-based Sybil Defenses**
Bimal Viswanath, Ansley Post, Krishna P. Gummadi, and Alan Mislove
SIGCOMM, New Delhi, India, August 2010

WSDM'10 **You Are Who You Know: Inferring User Profiles in Online Social Networks**
Alan Mislove, Bimal Viswanath, Krishna P. Gummadi, and Peter Druschel
WSDM, New York, NY, February 2010

WOSN'09 **On the Evolution of User Interaction in Facebook**
Bimal Viswanath, Alan Mislove, Meeyoung Cha, and Krishna P. Gummadi
WOSN, Barcelona, Spain, August 2009

GLOBECOM'07 **A Markov Chain Model for TCP NewReno over Optical Burst Switching Networks**
Bimal Viswanath, T. Venkatesh, and C. Siva Ram Murthy
GLOBECOM, Washington D.C, November 2007

Funding

2023 Title: “Defending Against Malicious LLM-Driven Agents Utilized for Online Abuse Directed at At-Risk Communities”
Sponsor: CCI
Team: PI: Bimal Viswanath (VT), Co-PIs: Yixin Sun (UVA), Lanfei Shi (UVA)
Total: $50,000, Personal share: $25,000 (50%)
Project time frame: 06/2024 — 05/2025
Status: Active

2023 Title: “SaTC: CORE: Small: Systematic Threat Characterization and Prevention in Open-Domain Dialog Systems”
Sponsor: NSF
Team: PI: Bimal Viswanath (VT), Co-PIs: Danfeng Yao (VT),
Total: $600,000, Personal share: $418,827 (69%)
Project time frame: 02/2023 — 01/2026
Status: Active

2023 Title: “Robust Classification of Adversarial Images from Generative AI Models”
Sponsor: CCI
Team: PI: Bimal Viswanath (VT), Co-PIs: Peng Gao (VT), Taejoong Chung (VT)
Total: $37,500, Personal share: $36,000 (96%)
Project time frame: 09/2023 — 06/2024
Status: Active

2023 Title: “Secure and Trustworthy Data and Technology: Evolution to a New Era”
Sponsor: 4-VA
Team: PI: Gretchen Matthew (VT), Co-PIs: Bimal Viswanath (VT)
Total: $30,000, Personal share: $12,000 (40%)
Project time frame: 07/2023 — 06/2024
Status: Active

2022 Title: “Securing the Interactions with AI-based Question- Answering Dialog Systems”
Sponsor: CCI
Team: PI: Bimal Viswanath (VT), Co-PIs: Megan Duncan (VT)
Total: $30,000, Personal share: $26,500 (88%)
Project time frame: 12/2022 — 06/2024
Status: Active

2022 Title: “High Accuracy Automatic Code Repair for Mission- critical Software”
Sponsor: CCI
Team: PI: Danfeng Yao (VT), Co-PIs: Bimal Viswanath (VT), Ismini Lourentzou (VT)
Total: $75,000, Personal share: $11,250 (15%)
Project time frame: 07/2022 — 06/2023
Status: Completed

2021 Title: “Assessing Specialty Crop Health and Quality using Machine Learning”
Sponsor: Virginia Tech
Team: PI: Song Li (VT), Co-PIs: Bimal Viswanath (VT), Chris North (VT)
Total: $60,000, Personal share: $14,000 (23%)
Project time frame: 04/2021 — 03/2022
Status: Completed

2020 Title: “Democratization of Data Breach and Data Loss Prevention Technologies and Knowledge”
Sponsor: Office of the Vice Provost for Learning Systems Innovation and Effectiveness, VT
Team: PI: Danfeng (Daphne) Yao (VT), Co-PIs: Tabitha James (VT), Tanu Mitra (VT), Bimal Viswanath, Idris Adjerid (VT)
Total: $20,000, Personal share: $2,500 (12.5%)
Project time frame: 01/2020 — 06/2020
Status: Completed

2020 Title: “System-wide Measurement of Defense-in-depth Readiness of Medical CPS Devices”
Sponsor: CCI South West Virginia
Team: PI: Danfeng (Daphne) Yao (VT), Co-PIs: Bimal Viswanath, Homa Alemzadeh (University of Virginia)
Total: $20,000, Personal share: $2,500 (12.5%)
Project time frame: Project time frame: 5/2020 — 12/2020
Status: Completed

2019 Title: “Faculty Mentoring Project Grant”
Sponsor: Office of the Provost, VT
Team: PI: Bimal Viswanath
Total: $1,500, Personal share: $1,500 (100%)
Project time frame: Project time frame: 3/2019 — 3/2021
Status: Completed

Professional Activities

Technical Program Committees

CCS	ACM Conference on Computer and Communications Security. 2021, 2022, 2023, 2024
NDSS	Network and Distributed System Security Symposium. 2020, 2021
USENIX Security	USENIX Security Symposium. 2020, 2021, 2022
ACSAC	Annual Computer Security Applications Conference. 2019, 2020, 2021
IMC	ACM Internet Measurement Conference. 2019
ICDCS	IEEE International Conference on Distributed Computing Systems. 2018, 2020
ICWSM	AAAI International Conference on Web and Social Media. 2015, 2016, 2017, 2018
COMSNETS	International Conference on Communication Systems & Networks. 2016, 2018

Reviewer for Journals

IEEE Network Special Issue	IEEE Network Special Issue on Online Social Network
IEEE TDSC	IEEE Transactions on Dependable and Secure Computing
IEEE/ACM ToN	IEEE/ACM Transactions on Networking
ACM TSC	ACM Transactions on Social Computing

Patents

2018 **Method for Assessing Host and Deployment Reliability in Data Centers**
Istemi Ekin Akkus, Ivica Rimac, Ruichuan Chen, Bimal Viswanath, and Volker Hilt
Europe Patent No. EP3244570, granted on 12/12/2018

Talks

Invited Talks

2023 *"Investigating Foundation Models Through the Lens of Security"*
- Distinguished CS Speaker series, University of Virginia, VA, November 2023

2023 *"Investigating Foundation Models Through the Lens of Security"*
- CyberAI Winter School, University of Texas at San Antonio, Austin, TX, November 2023

2023 *"Studying Large Language Models Through the Lens of Security: Defending Against Misuse and Vulnerabilities"*
- ARO Workshop on AI for Security, Arlington VA, January 2023

2022 *"Studying Large Language Models Through the Lens of Security: Defending Against Misuse and Vulnerabilities"*
- CCI Integrated Security Seminar, Virginia Tech, Blacksburg VA, November 2022

2022 *"Fighting Evolving Deepfake Threats"*
- Wireless Telecommunications Symposium (WTS), Online, April 2022

2021 *"Understanding and Defending Against Deepfake Threats"*
- Department of Computer Science, University of Iowa, online, June 2021

2020 *"Defending Against the Malicious Use of AI"*
- CS Alumni Webinar at Virginia Tech, online, September 2020
- School of Plant and Environmental Sciences at Virginia Tech, online, November 2020

2018 *"Security in an AI-driven World"*
- Virginia Tech, Department of Computer Science, March 2018
- University of British Columbia, Department of Computer Science, March 2018
- University of Iowa, Department of Computer Science, March 2018
- University of Rochester, Department of Computer Science, April 2018
- Indiana University-AFRL Workshop, Bloomington, IN, May 2018

2015 *"Strength in Numbers: Robust Tamper Detection in Crowd Computations"*
- Yelp Security Team, San Francisco, CA, USA, November 2015

2015 *"Towards Trustworthy Social Computing Systems"*
- NEC Laboratories Europe, Heidelberg, Germany, March 2015
- Bell Labs, Stuttgart, Germany, March 2015
- Microsoft Research India, Bangalore, India, April 2015
- Telefonica Research, Barcelona, Spain, May 2015

2012 *"Understanding and Combating Link Farming in the Twitter Social Network"*
- Réseaux et individus, Informatique et sciences sociales, Paris-Diderot University, Paris, France, November 2012

Selected Press

10/2023 *“Artificial intelligence: What are the risks and benefits?”*, PBS

10/2023 *“Curious Conversations”*, Office of Research and Innovation at Virginia Tech

07/2023 *“The Rise of the Chatbots”*, CACM

05/2023 *“Virginia Tech research aims to reduce toxic language from artificial intelligence”*, WDBJ7

04/2023 *“The chatbot whisperers”*, VT News

11/2022 *“The strengths and limitations of approaches to detect deepfake text”*, TechXplore

10/2017 *“Could AI Be the Future of Fake News and Product Reviews?”*, Scientific American

09/2017 *“Many People Can’t Tell The Difference Between Yelp Reviews Written By An AI And A Human. Can You?”*, Forbes

09/2017 *“AI writes Yelp reviews that pass for the real thing”*, Engadget

09/2017 *“The potential of AI generated ‘crowdturfing’ could undermine online reviews and dramatically erode public trust”*, News.com.au

08/2017 *“Researchers taught AI to write totally believable fake reviews, and the implications are terrifying”*, Business Insider

08/2017 *“Restaurant Reviews Could Be Generated By AI Without You Noticing”*, Yahoo News

08/2017 *“AI Writes Believable Fake Yelp Reviews”*, NVIDIA Developer

08/2017 *“AI trained on Yelp data writes fake restaurant reviews ‘indistinguishable’ from real deal”*, The Verge

08/2017 *“Robots learned how to write fake Yelp reviews like a human”*, New York Post

10/2016 *“Using Google Chrome as your preferred browser? Think again”*, Economic Times, India

04/2015 *“The Bot Bubble: How click farms have inflated social media currency”*, New Republic

04/2012 *“Who’s to blame for Twitter spam? Obama, Gaga and you”*, GigaOM

03/2011 *“Privacy: Facebook’s Achilles heel”*, CNET News

03/2010 *“On Social Networks, You Are Who You Know”*, Slashdot

Teaching Experience

Instructor, CS6604 Advanced Topics in Data and Information, Virginia Tech, Spring 2024

Instructor, CS4274 Secure Computing Capstone, Virginia Tech, Fall 2021, Spring 2023, Spring 2024

Instructor, CS5914 Security Risks of Generative AI, Virginia Tech, Fall 2023

Instructor, CS5914 Defending Against ML-powered Adversaries, Virginia Tech, Fall 2022

Instructor, CS6604 Topics in Security and AI, Virginia Tech, Spring 2020, Spring 2022

Instructor, CS5984 Security Analytics, Virginia Tech, Spring 2019, Spring 2021

Instructor, CS4254 Network Architecture and Programming, Virginia Tech, Fall 2018, Fall 2019, Fall 2020

Instructor, Readings in Social Computing Systems, Saarland University, Summer 2013

Current Research Advisees

- *Aravind Cheruvu*, PhD at VT CS, Expected Completion date: 2026
- *Sifat Muhammad Abdullah*, PhD at VT CS, Expected completion date: 2025

- *Shravya Kanchi*, PhD at VT CS, Expected completion date: 2026
- *Nicholas Kong*, MS at VT CS, Expected completion date: 2024.

Graduated Advisees

- *Connor Weeks*, MS at VT CS, Completion date: May 2023.
- *Jiameng Pu*, PhD at VT CS, Thesis title: "Defending Against Misuse of Synthetic Media: Understanding Real-world Challenges and Building Robust Defenses", Completion date: September 2022.
- *Cristian Vives*, MS at VT CS. Thesis title: "NoiseLearner: An Unsupervised, Content-agnostic Approach to Detect Deepfake Images", Completion date: February 2022
- *Kavya Sundaram*, Undergraduate researcher at VT CS.
- *Steve T K Jan* (co-advised with Gang Wang), PhD at VT CS, Thesis title: "Robustifying Machine Learning based Security Applications", Completion date: August 2020.
- *Ahmadreza Azizi*, MS at VT CS, Thesis title: "Defending Against Trojan Attacks on Neural Network-based Language Models", Completion date: May 2020.
- *Tianrui Hu*, MS at VT CS, Thesis title: "Detecting Bots using Stream-based System with Data Synthesis", Completion date: May 2020. Next step: PhD program at Northeastern University.
- *Neal Mangaokar*, Undergraduate researcher at VT CS, won the 2020 David Heilman Researcher Award from VT CS. Next step: PhD program at the University of Michigan.
- *Lauren Kelly*, Undergraduate researcher at VT CS. Next step: IT Software Engineer, University of North Florida.