

Sunil Manandhar

sunil@ibm.com | +1(757) 345-9788 | <https://linkedin.com/in/sunil-manandhar> | <https://sunilmanandhar.com>

RESEARCH

I am a Security and Privacy Research Scientist at IBM T.J. Watson Research Center. I received my Ph.D. from William & Mary. My research interests include IoT security, privacy, software security, and NLP. I completed my B.Sc. in Computer Science and Information Technology from St. Xavier's College, Nepal.

EDUCATION

Ph.D. in Computer Science, GPA 3.85 - **The College of William and Mary**, Williamsburg, VA *Aug 2016 - Aug 2022*

Advisor: [Dr. Adwait Nadkarni](#)

Relevant Coursework: Advanced System Security Engineering, Advanced Topics in System and Security, CyberSecurity Research Analysis, Computer & Network Security, Advanced Software Engineering, Ubiquitous and Mobile Computing, Analysis of Algorithms, Intro to Machine Learning

BS in Computer Science and IT, GPA: 79.5% - **Tribhuvan University**, Kathmandu, Nepal *Nov 2011 - Nov 2015*

PUBLICATIONS

X. Jin*, **Sunil Manandhar***, Kaushal Kafle, Z. Lin, and Adwait Nadkarni, "Understanding IoT Security from a Market-Scale Perspective," in Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, USA, 2022. *Co-first Authors., To appear. [[PDF](#) | [Artifact](#)]

Sunil Manandhar, Kaushal Kafle, B. Andow, K. Singh, and **Adwait Nadkarni**, "Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage," in *Proceedings of the 31st USENIX Security Symposium (USENIX)*, Boston, MA, USA, 2022. Accepted, to appear. [[PDF](#) | [Data](#)]

Kaushal Kafle, Kevin Moran, **Sunil Manandhar**, Adwait Nadkarni, and Denys Poshyvanyk. Security in Centralized Data Store-based Home Automation Platforms: A Systematic Analysis of Nest and Hue. *ACM Transactions on Cyber Physical Systems, special issue on Security and Privacy for Connected CPS (TCPS)* [[PDF](#)]

Sunil Manandhar, Kevin Moran, Kaushal Kafle, Ruhao Tang, Denys Poshyvanyk, and Adwait Nadkarni. Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses. *To Appear in the Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P)*, San Francisco, CA, USA, May 2020. [[PDF](#) | [CODE](#)]

Kaushal Kafle, Kevin Moran, **Sunil Manandhar**, Adwait Nadkarni, and Denys Poshyvanyk. A Study of Data Store-based Home Automation. *In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Dallas, TX, USA, March 2019. **Best Paper Award**. [[Press Coverage](#)] [[PDF](#)]

Sigmund Albert Gorski III, Ben Andow, Adwait Nadkarni, **Sunil Manandhar**, William Enck, Eric Bodden, and Alexandre Bartel. ACMiner: Extraction and Analysis of Authorization Checks in Android's Middleware. *In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Dallas, TX, USA, March 2019. [[CVE-2019-9351](#), [CVE-2019-9377](#), [CVE-2019-9438](#)] [[PDF](#)]

WORK EXPERIENCE

Research Scientist, Security and Privacy, IBM Research

August 2022-

- ❑ Zero Trust Security
- ❑ Policy Analysis

COVES Fellow, Center for Innovative Technology*May 17 2021- Aug 06 2021*

- ❑ Model statewide privacy policies for Smart Community Testbed (ongoing)
 - ❑ Systematic Literature Review on privacy challenges in Smart Cities
 - ❑ Interaction with Testbed Technologist and State/County officials

Co-op, IBM*Sep 2020 - Dec 2020*

- ❑ Privacy Compliance Framework
 - ❑ Created pipeline for NLP tasks to automate information extraction from privacy regulation and privacy policy
 - ❑ Trained Named-Entity-Recognition (NER) Model to extract data objects and entities from privacy policy
 - ❑ Multi Label Classification using BERT

Research Intern, IBM*Jun 2020 - Sep 2020*

- ❑ Framework for Privacy Policy analysis
 - ❑ Worked on extraction of entities and relation to understand information flow in privacy policies
 - ❑ Analysis of Privacy Policy using existing tools and techniques

Lead Grad Student, SPL Lab*Jan 2020 - Present*

- ❑ Conducted weekly student-run meetings and organized events to improve research skills
- ❑ Managed lab website and logistics [[Website](#)]
- ❑ Mentored 4 students in research projects

Research Assistant, CS Department, William & Mary*May 2018 - Present*

- ❑ Designed framework for Regulation Analysis
- ❑ Analyzed Privacy Policies to develop insights into data protection practices
- ❑ Designed framework for generating natural home automation scenarios to improve security and safety in smart homes
- ❑ Developed proof of concept exploits for vulnerabilities in access control enforcement of APIs in the Android Platform

Teaching Assistant, William & Mary*Aug 2016 - May 2017*

- ❑ Computational Problem Solving

Technology Lead, Universal Language Learning, China*Dec 2016 - Present*

- ❑ Built a chatbot engine for kids to help with language learning. <https://my-little-harper.myshopify.com/>

Mobile App Developer, Moondrop, San Francisco*Jan 2016 - Aug 2016*

- ❑ Managed Mobile Application and Updated the App with Material Design <https://tinyurl.com/y65eafd6>

Software Engineer, Bajra Technologies, Kathmandu, Nepal*Jan 2015 - Jan 2016*

- ❑ SiteHawk - Crawler, and Interface for Website Site Deface Detection <https://tinyurl.com/y4ro377>
- ❑ Imperial - Cordova based Mobile App for Side-Kick Plus Device <https://tinyurl.com/y6dz3qjg>

Business Associate, Axon System, Kathmandu, Nepal*May 2014 - Dec 2014*

- ❑ MyFarm - Mobile Application
- ❑ Driving License Mobile App <https://tinyurl.com/s6rjgmo>

AWARDS AND HONORS

- ❑ [International Student Achievement Award](#) - Reves Center, 2022
- ❑ [NSF CPS-Cyber-Physical Systems Grant](#)
 - ❑ Title: “Enabling Data-Driven Security and Safety Analyses for Cyber-Physical Systems”
 - ❑ PI: Adwait Nadkarni, Kevin Moran, Co-Pi: Denys Poshyvanyk, Contributor: **Sunil Manandhar**
 - ❑ Award CNS-2132281, totaling \$799,839
- ❑ [COVA CCI](#) Cyber Security Dissertation Fellowship

- ❑ Title: “Improving Privacy, Security, Safety in Emerging Platforms”
 - ❑ PI: Adwait Nadkarni, Graduate Fellowship: **Sunil Manandhar**
 - ❑ Award Grant: 759381, totaling \$25,000
- ❑ [The Commonwealth of Virginia Engineering & Science \(COVES\) Fellow](#), 2021
- ❑ [S. Laurie Sanderson Award for Excellence in Undergraduate Mentoring Award](#), 2021
- ❑ [Distinguished Reviewer](#) - Shadow PC, IEEE S&P 2021
- ❑ Best Paper Award at CODASPY, Dallas, TX, USA, March 2019
- ❑ Received 3 CVEs and mentions on the Android Security Bulletin
- ❑ Winner of Imagine Cup Nepal 2014
- ❑ Winner of Skype Challenge in Imagine Cup 2014
- ❑ President of Computer Science and Information Technology Association of Nepal (2014)
- ❑ Microsoft Student Partner - St. Xavier’s College (2014)

PRESENTATIONS AND INVITED TALKS

- ❑ “Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses”
 - ❑ 41st IEEE Symposium on Security and Privacy
 - ❑ IBM
 - ❑ Journal Club, William & Mary
- ❑ “Outlier Detection in Large Scale Dataset”
 - ❑ 17th Annual Graduate Research Symposium

PROFESSIONAL SERVICE

- ❑ **Reviewer for ACM WiSec '21 Replicability Evaluation Committee**
- ❑ **Shadow PC for IEEE S&P '21**
- ❑ **Sub-reviewer for Conferences**
 - ❑ USENIX Security Symposium (USENIX) '19, '21
 - ❑ USENIX Safethings 2021
 - ❑ ISOC Network and Distributed System Security Symposium (NDSS), '20,'22
 - ❑ The International Conference on Information Systems Security (ICISS), '19
- ❑ **Student Technology Advisory Committee (Arts and Science Department - William & Mary) ('20)**