

Hasini Gunasinghe

@hasi7786@gmail.com ☎ 001-765-714-9268

in www.linkedin.com/in/hasinitg 📄 Google Scholar

Education









- **Ph.D. in Computer Science** Fall 2013 – Summer 2021
Purdue University West Lafayette, IN, USA
- **M.S. in Computer Science** Fall 2013 – Spring 2016
Purdue University West Lafayette, IN, USA
- **B.Sc. (First-Class Honours) in Computer Science and Engineering** May 2006 – Sept 2010
University of Moratuwa Moratuwa, Sri Lanka

Industry Experience

- **Google Inc., Mountain View, CA, USA** April 2020 – Present
Software Engineer - Android Security and Privacy Team
 - Contributed to the design and development of the following key security features to the [Android operating system](#) and the eco system, which is used by over 3 billion users world wide.
 - * Keystore - a central component in the Android operating system which provides hardware backed cryptographic services to the Android applications and other system components.
 - * Device Identifier Composition Engine (DICE) chain for the Android Virtualization Framework (AVF) - enables a protected virtual machine (PVM) running in the AVF to obtain hardware backed cryptographic secrets and a verifiable identity.
 - * Keymint - the reference implementation of the hardware backed cryptographic engine running in Android devices.
 - Contributed to finding/reporting/fixing security vulnerabilities in the components owned by the Android Hardware backed Security team.
 - **IBM T. J. Watson Research Center, Yorktown Heights, NY, USA** May 2017 – Aug. 2017
Research Intern - Information Security Team
 - Designed and developed a protocol for privacy preserving and secure exchange of digital identity assets in a decentralized identity management ecosystem backed by a permissioned blockchain. [📄](#) [🔗](#)
 - **Salesforce.com, San Francisco, CA, USA** May 2016 – Aug. 2016
Software Engineering Intern - Infrastructure Security Team
 - Contributed to the development of next generation access control solution for Salesforce data centers.
 - **WSO2 Inc., Sri Lanka** Sept 2010 – May 2013
Software Engineer - Security and Identity Management Team
 - Designed and implemented the following features for the [WSO2 Identity Server](#), which is an open source digital identity management solution, currently used by over 1500 organizations world wide with over a billion identities under management.
 - * The standardized identity provisioning based on the open standard named SCIM (System for Cross-domain Identity Management) and integration of SCIM with OAuth2.0.
 - * The LDAP (Light Weight Directory Access Protocol) based user and access management with support for multi-tenancy.
 - Represented WSO2 in the first SCIM interoperability event at the IETF (Internet Engineering Task Force) 83rd meeting held in Paris, France in March 2012. [🔗](#)
 - On-site customer support engagements conducted in the USA and Germany.
 - Co-conducted a pre-conference tutorial on the topic: *Enterprise Security and Identity Management with WSO2 Identity Server* at the WSO2Con 2013 held in London, UK. [🔗](#)
 - Managed two releases of WSO2 Identity Server (3.2.3 and 4.0.0) as the release manager.
-

Research Experience




Designed and developed secure and privacy preserving online protocols for real world use cases, with special focus on digital identity management. Selected research projects:

- **PEBASI:** An efficient online biometric authentication scheme which protects users' biometric privacy from service providers and transaction privacy from identity providers. Different from traditional identity provider-centric authentication model, PEBASI is based on a user-centric authentication model. At the heart of the scheme is a novel biometric matching technique which *outperforms the state-of-the-art by 35% in terms of end-to-end execution time*, which is based on a novel hybrid secure multiplication framework. 
- **PrivIdEx:** A protocol enabling service providers to exchange users' verified identity information over a decentralized identity management platform backed by a permissioned blockchain network. The protocol makes identity verification scenarios such as *KYC (Know Your Customer)*, more convenient and less expensive. It preserves both security (e.g. correctness, ownership assurance, protection from counterfeits, financial fairness) and privacy (e.g. confidentiality, anonymity, unlinkability) properties which are conflicting yet critical requirements. Zero knowledge proofs combined with other cryptographic tools in unique ways achieve these conflicting requirements in the decentralized setting.  
- **PrivBioMTAuth:** The first user-centric biometric authentication protocol enabling privacy preserving remote authentication from mobile phones. The main building blocks are zero knowledge proofs (ZKP) and machine learning classification. An approach protecting the ZKP protocols from mafia attacks is proposed as an independent contribution.  
- **RahasNym:** A pseudonymous identity management system supporting unlinkable and accountable online transactions. A policy language combined with light weight cryptography makes it efficient for online transactions.   

Publications

- **Conference Papers and Presentations:**
 - H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh, D. Song. **PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets.** The World Wide Web Conference (WWW) 2019, San Francisco, CA, USA. (*acceptance rate: 18%*) 
 - H. Gunasinghe, E. Bertino. [Invited Paper] **RahasNym: Pseudonymous Identity Management System for Protecting against Linkability.** The 2nd IEEE International Conference on Collaboration and Internet Computing, CIC 2016, Pittsburgh, PA, USA. 
 - H. Gunasinghe, E. Bertino. [Poster Paper] **RahasNym: Protecting against Linkability in the Digital Identity Ecosystem.** The 35th IEEE International Conference on Distributed Computing Systems, ICDCS 2015, Columbus, OH, USA, June 2015. 
 - H. Gunasinghe, E. Bertino. **Privacy Preserving Biometrics-Based and User Centric Authentication Protocol.** The 8th International Conference in Network and System Security, NSS 2014, Xian, China. 
- **Journal Papers:**
 - H. Gunasinghe, E. Bertino. **PrivBioMTAuth: Privacy Preserving Biometrics-Based and User Centric Protocol for User Authentication from Mobile Phones.** IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, p. 1042-1057, April, 2018. (*impact factor: 7.231*) 
 - H. Gunasinghe, M. Atallah, E. Bertino. **PEBASI: A Privacy preserving, Efficient Biometric Authentication Scheme based on Irises.** In submission.

Patents

- S. Chari, H. Gunasinghe, H.M. Krawczyk, A. Kundu, K. K. Singh, D. Su. **Protection of Confidentiality, Privacy and Ownership Assurance in a Blockchain Based Decentralized Identity Management System.** U.S. Patent 10 833 861, Nov. 10, 2020. 
- S. Chari, H. Gunasinghe, A. Kundu, K. K. Singh, D. Su. **Protection of confidentiality, privacy and financial fairness in a blockchain based decentralized identity management system.** U.S. Patent 10 715 317, Jul. 14, 2020. 
- S. Chari, H. Gunasinghe, A. Kundu, K.K. Singh, D. Su. **Privacy-preserving identity asset exchange.** U.S. Patent 10 944 560, Mar. 14, 2020. 

¹The link is from a web archive because IEEE computer society has moved from IEEE Computing Now to IEEE Tech News 

Volunteered Professional Services

- Conducted a technical talk on “Zero Knowledge Proof Protocols” to the Android Hardware backed Security team at Google Inc. (*January 2022*).
 - Conducted a guest lecture on “Zero knowledge proofs and their applications in digital identity management” in the seminar course on Data Security and Privacy (CS 59000-DSP) at Purdue University (*Spring 2019*).
 - Served as a reviewer/sub reviewer for the following renowned journals and conferences:
 - Journals:
 - * IEEE Transactions on Information Security and Forensics 2018-2019
 - * IEEE Transactions on Dependable and Secure Computing 2014-2019
 - Conferences:
 - * The ACM World Wide Web Conference (WWW) 2019
 - * The IEEE International Conference on Distributed Computing Systems (ICDCS) 2019
 - * The ACM Symposium on Access Control Models and Technologies (SACMAT) 2015
 - * The ACM ASIA Conference on Computer and Communications Security (AsiaCCS) 2014, 2015
 - * The ACM Conference on Data and Application Security and Privacy (CODASPY) 2015, 2018
 - Volunteered visiting instructor at University of Moratuwa (2009-2010).
-

Teaching Experience

- Served as a Graduate Teaching Assistant for the following courses offered by Purdue University (*Jan 2015 - May 2018*):
 - Software Engineering (CS 307)
 - Senior Software Engineering (CS 407)
-

Awards

- **Research Awards and Recognitions:**
 - Best Poster Paper Award in the 35th IEEE International Conference on Distributed Computing Systems, Columbus, OH, USA, June 2015.
 - Emil Stefanov Memorial Fellowship for originality and creative thinking in security research in 2019. [↗](#)
 - IBM PhD Fellowship in 2018. [↗](#) [↗](#)
 - Bisland Dissertation Fellowship awarded by the Graduate School, Purdue University in 2019.
 - The paper titled: “RahasNym: Pseudonymous Identity Management System for Protecting against Linkability” was featured in IEEE Computing Now under the theme: *Improving Cybersecurity: User Accountability and Sociotechnical Systems* in April 2017 [↗](#)¹.
 - Research funding was awarded by the Google ATAP program [↗](#) for the proposal titled: “Privacy Preserving Multimodal Biometrics-based Continuous Authentication System for Smart Phones” in 2015.
 - Summer Research Grant awarded by the Graduate School, Purdue University in 2018.
 - Best Paper Award in the 8th International Conference on Network and Systems Security, China, 2014.
- **Industry Awards and Recognitions:**
 - Outstanding Contributor Award by WSO2 Inc. for the year 2011.
 - Outstanding Contributor Award by WSO2 Inc. for the year 2012.
 - Listed in the Android Security Acknowledgements in January 2021 by the Android Security Team for finding, reporting and fixing the CVE-2021-0320 [↗](#).
 - Second Runners-Up in the Software Design Category of Imagine Cup 2008, which is an island wide competition organized by Microsoft, Sri Lanka [↗](#).

¹The link is from a web archive because IEEE computer society has moved from IEEE Computing Now to IEEE Tech News [↗](#)

- **Academic Awards:**

Placement in the Dean's List for academic excellence, University of Moratuwa, Sri Lanka (2006 to 2010).

- **Teaching Awards:**

- Raymond Boyce Graduate Teacher Award by the Computer Science Department, Purdue University in 2017, which is listed in the department's hall of fame.
- Graduate Teaching Assistant Award (sponsored by Harris Corporation) by the Computer Science Department, Purdue University in 2016.

- **Travel Grants:**

- Travel grant awarded by Purdue University to attend the Grace Hopper Women in Computing in 2016.
- Travel grant awarded by the National Science Foundation (NSF) to attend the Summer School on Secure Computation in 2016.
- Travel grant awarded by NSF to attend IEEE ICDCS in 2015.
- Travel grant awarded by the ZKProof Steering Committee to attend the 2nd ZKProof Workshop in 2019.

Contributions to Open Source and Open Standards

- Initiated and released the first version of the open source project: WSO2 Charon, as the sole contributor in 2012 [↗](#) [↗](#). WSO2 Charon is one of the first implementations of the open standard: SCIM, released under Apache 2.0 licence [↗](#), which successfully interoperated with the other implementations of SCIM at the first SCIM interoperability event at the IETF 83rd meeting held in Paris, France in March 2012 [↗](#). Now it has grown to a project with 72 contributors.[↗](#)
- Contributed to the SCIM Standardization Working Group in 2012. [↗](#)
- Successfully completed a Google Summer of Code (GSoC) project by designing and implementing an access control solution for Apache Airavata project in GSoC 2015. Earned the committership in the Apache Software Foundation for the Airavata Project. [↗](#) [📄](#)
- Contributed platform security features to the Android operating system and Trusty - which is the secure operating system that provides a Trusted Execution Environment (TEE) for Android. [↗](#)
- Contributed to the open source identity and access management solution: WSO2 Identity Server (2010 - 2013).