

Ruchith Fernando

Department of Computer Science
Purdue University
305 N. University Street
West Lafayette, IN 47907

rfernand@purdue.edu
www.ruchith.org

- EDUCATION **Purdue University**, West Lafayette, IN Aug 2014 (expected)
Ph.D. in Computer Science
- Purdue University**, West Lafayette, IN May 2012
M.Sc. in Computer Science
- University of Moratuwa**, Colombo, Sri Lanka Nov 2004
B.Sc. in Computer Science and Engineering
- PUBLICATIONS **Privacy-Preserving Authentication Using Service Provider Policies with Credential Relationships**,
Ruchith Fernando, Bharat Bhargava
Submitted for Review, June 2014
- Incorporating Attacker Capabilities in Risk Estimation and Mitigation**, Lotfi ben Othmane, Rohit
Ranchal, Ruchith Fernando, Bharat Bhargava, Eric Bodden
Submitted for Review, January 2014
- Likelihood of Threats to Connected Vehicles**, Lotfi ben Othmane, Ruchith Fernando, Rohit Ranchal,
Bharat Bhargava, Eric Bodden
Submitted for Review, January 2014
- Private Anonymous Messaging**, Ruchith Fernando, Bharat Bhargava, Mark Linderman
IEEE Symposium on Reliable Distributed Systems, 2012
- Aggregated Privacy-Preserving Identity Verification for Composite Web Services**, Nan Guo,
Tianhan Gao, Bin Zhang, Ruchith Fernando, Elisa Bertino
IEEE International Conference on Web Services, 2011
- Privacy Preserving Identity Attribute Verification in Windows CardSpace**, Kevin Steuer Jr.,
Ruchith Fernando, Elisa Bertino
ACM workshop on Digital Identity Management, 2010
- A modular Architecture for Secure and Reliable Distributed Communication**, Chamikara Jayalath
and Ruchith Fernando
International Conference on Availability, Reliability and Security, 2007
- Using Blood Glucose Data as an Indicator for Epidemic Disease Outbreaks**, Eirik rsand, Ole Anders
Walseth, Niklas Andersson, Ruchith Fernando, Ove Granberg, Johan G. Bellika, Gunnar Hartvigsen
Medical Informatics Europe , 2005
- SecureZone: A Framework for WS - Secure Conversation and WS - Trust**, Ruchith Fernando,
Dimuthu Leelarathne, Malinda Kaushalye
International Information Technology Conference, Sri Lanka, 2004
- POSTERS **A Framework for Service Activity Monitoring**, Ruchith Fernando, Rohit Ranchal, Pelin Angin,
Raghav Shankar, Bharat Bhargava
CERIAS Symposium, 2014

Sustainable Secure Data Dissemination in Distributed Environments, Rohit Ranchal, Ruchith Fernando, Bharat Bhargava
IFIP Conference on Sustainable Internet and ICT for Sustainability, Italy, 2013

Unlinkable Complex Identity Claims, Ruchith Fernando, Bharat Bhargava
CERIAS Symposium, 2013

Private Anonymous Messaging, Ruchith Fernando, Bharat Bhargava
CERIAS Symposium, 2012
Honorable mention(4th place) at the poster competition

ACADEMIC AWARDS	Honorable Mention, Research Poster Competition, 13th Annual Information Security Symposium, CERIAS	2012
	Best Final Year Project Student Computer Science and Engineering, University of Moratuwa, Sri Lanka	2005
	Dean's list, 3 semesters, University of Moratuwa, Sri Lanka	2001 - 2004

RESEARCH EXPERIENCE **Service Monitoring Framework**
Designed and implemented a framework to monitor and analyze SOA deployment patterns. This includes development of an active policy (XACML) based interaction control module.
<https://code.google.com/p/end-to-end-soa/>

AnonIDM
Designed and implemented an anonymous and unlinkable credential system where a user's interactions with a service provider can be made unlinkable while ensuring the user satisfies complex authentication policies of the service provider. This scheme further allows the presence of an off-line identity provider.
<https://code.google.com/p/anon-idm/>

Anon Encrypt
Designed and implemented of an encryption scheme, which modifies hierarchical identity based encryption, to provide new privacy and anonymity features for P2P information sharing.
<https://code.google.com/p/anon-encrypt/>

Secure Data Sharing and Access Control in Distributed Environments
Co-developed a framework to adapt and experiment the concept of *Active Bundles* in SOA environments.
<https://code.google.com/p/absoa/>

VeryIDX
Designed and implemented a standard Web services interface for the challenge response protocol of the zero knowledge proof of knowledge of identity attributes and the aggregate signature scheme. Extended a Microsoft CardSpace Identity Provider to issue unlikable security tokens for proof of knowledge of identity attributes and implemented the relying party components to carryout the proof.

PROFESSIONAL EXPERIENCE	Rosen Center for Advanced Computing , Purdue University, IN Software Engineer	Aug 2008 – Present
	Designed and implemented the core HUBzero database technologies for web-forms data contribution, processing, and validation. This is used across 10 medical and scientific databases across 8 Hubs. This work further included implementing data encryption to comply with HIPPA regulations.	
	Member of the <i>Infusion Pump Informatics</i> system development team responsible for processing smart pump device output, administration component, authorization framework, analysis charts/reports and dashboard.	
	Developed the data extraction capabilities for <i>International Breast Cancer and Nutrition</i> project where a user is allowed to scrape content from a complex web application to extract DNA modification and experiment data.	

Wize Commerce Inc., San Mateo, CA

Platform Engineer Intern

May 2013 – Aug 2013

Developed a feature set and a machine learning model to identify rogue bots that scrapes content from web applications. The experimental model was able to classify rogue bots with 90% accuracy.

Qualcomm Inc., San Diego, CA

Interim Engineering Intern

May 2011 – Aug 2012

Researched privacy preserving sensor data contribution for collaborative analysis in context aware applications.

WSO2 Inc., Colombo, Sri Lanka

Technical Lead and Product Manager

Jun 2005 – Aug 2008

Implemented the Web service security specifications for Apache Axis2 in the form of the Apache Rampart project. Actively contributed to Apache AXIOM, Apache WSS4J projects. Member of the Web Services Application Server development team responsible for the web services security components. Designed and led the development team of WSO2 Identity Server. Carried out on-site and online customer training programs on Web services security, Apache and WSO2 Web services frameworks. Represented WSO2 and Apache Software Foundation at interoperability workshops and successfully completed all Web service security interoperability scenarios. Published a host of tutorials and articles on the WSO2 developer portal.

Apache Software Foundation

Committer/Project Management Committee Member/Member

2005 – Present

Contributed to the Apache Web services projects (Axis2/AXIOM/WSS4J) and founded the Apache Rampart project.

Eurocenter DDC, Colombo, Sri Lanka

Software Engineer

Dec 2004 – Apr 2005

Developed proof of concept applications for a pre-sales project as a member of the R&D department.

Norwegian Centre for Telemedicine, Tromsø, Norway

Software Engineer Intern

Aug 2004 – Dec 2004

Member of the research team to investigate the use of blood glucose data for epidemic disease outbreak detection.

Virtusa Pvt Ltd., Colombo, Sri Lanka

Software Engineer Intern

Jun 2003 – Dec 2003

Designed and developed a portal product evaluation tool for the R&D department and a member of the development team of the corporate knowledge management portal.

**OTHER
EXPERIENCE**

External mentor of final year undergraduate project (CS 420) at Computer Science and Engineering department, University of Moratuwa, Sri Lanka

Mentor, Google Summer of Code 2007 Representing Apache Software Foundation

Mentor, FOSSCode 2006 Representing Apache Software Foundation

Represented WSO2 Inc. at WS-SX Technical Committee of Organization for the Advancement of Structured Information Standards (OASIS) and WS-Policy Working Group of World Wide Web Consortium (W3C)

SKILLS

Java, PHP, JavaScript/Node.js, C, SQL

SOAP/WS-Sec*, XML-Security, Apache Web services

Pairing Based Cryptography

Machine Learning

Subversion, Git

Linux, Windows