

Sridhar Adepu

CONTACT INFORMATION	President Graduate Fellow Information Systems Technology and Design Singapore University of Technology and Design <i>Advisors:</i> Prof. Aditya Mathur and Prof. Jianying Zhou	<i>Mobile:</i> (+65)-8150 7386 adepu_sridhar@mymail.sutd.edu.sg
AREAS OF INTEREST	Cyber Physical Systems Security, Industrial Control Systems Security, Critical Infrastructure Protection and IoT security	
EDUCATION	Singapore University of Technology and Design , Singapore PhD, Information Systems Technology and Design, 2016 to December 2020 Courses Taken: Computer Networks, Theory and Application of Software Security, Analysis of Algorithms, Statistics and Machine Learning, Systems & Control and Models of Software Systems National Institute of Technology , Rourkela, India M.Tech., Computer Science and Engineering, 2011 to 2013 Courses Taken: Cryptographic Foundations, Network Security, Software Testing, Software Design, Pattern Recognition. Kakatiya University , Warangal, India B.Tech., Computer Science and Engineering, 2007 to 2011	
AWARDS AND ACHIEVEMENTS	<ul style="list-style-type: none">• Singapore National Blockchain Challenge Gold medal award for ‘BlockOps’ in 2019.• ASEAN ICT Gold medal award in research and development, 2018• Best paper award in SecCPS workshop 2017.• Best student paper award in HASE 2017.• Awarded finalist of the CIPRNET Young Critis Award CYCA (European Union)2016.• President’s graduate Fellowship award (2016 to 2021)• Best Teacher award in Vignan University for 2013-14.• First Position in the technical quiz context in RENDEVOUS’09, Warangal, 2009.• Under Graduate scholarship-2007, Government of Andhra Pradesh, India• School level Prathibha Puraskar Award, Board of Secondary Education, 2005.	
RESEARCH AND TEACHING EXPERIENCE	Visiting PhD student at Computer Science, Carnegie Mellon University, USA (July 2019 to August 2020) Advisors: Prof. Eunsuk Kang and Prof. David Garlan Applying formal methods to Cyber Physical Systems security. Teaching Assistant in Information Systems Technology and Design@SUTD 50.002 Computation Structures: Sept - Dec 2017. 50.003 Elements of Software Construction: Jan - April 2018. 50.577 Cyber Physical Systems Security: Jan - April 2018, 2019, 2020.	

iTrust, Centre for Research in Cyber Security, SUTD

Research Assistant, February, 2015 - August, 2016

Supervisor: Prof. Aditya P Mathur

- Developing an attack models and attack detection methods for cyber-physical systems.
- Impact and response analysis across interconnected infrastructures.
- I have contributed to iTrust in various aspects: managing testbeds, developing tools to communicate with testbeds, writing research grants, working with various government agencies to develop critical infrastructure protection

Vignan University, Guntur, India: *Lecturer*, June, 2013 - September, 2014

Courses: Data Structures, Theory of Computation, Software Engineering, Cyber Security.

Thesis Mentored: Six Undergraduate and One Masters dissertation Projects

Additional Responsibilities: Conducting laboratories, organizing workshops and seminars

PUBLICATIONS

To be published

- [1] **Sridhar Adep**, Nianyu Li, Eunsuk Kang and David Garlan "Modeling and Analysis of Explanation for Secure Industrial Control Systems" ACM Transactions on Autonomous and Adaptive Systems (submitted).
- [2] Zheng Yang, **Sridhar Adep**, Chenglu Jin and Jianying Zhou, "HMAKE: Legacy-Compliant Multi-factor Authenticated Key Exchange from Historical Data", in IEEE Internet of Things Journal (submitted).
- [3] **Sridhar Adep**, Aditya Mathur, " SafeCI: Avoiding Process Anomalies in Critical Infrastructure" in International Journal of Critical Infrastructure Protection (IJCIP) (Under second revision).

Published

- [4] **Sridhar Adep**, Venkata Reddy Palleti, Gyanendra Mishra, and Aditya Mathur. "Investigation of cyber attacks on a water distribution system." In International Conference on Applied Cryptography and Network Security, pp. 274-291. 2020.
- [5] Tanmoy Kanti Das, **Sridhar Adep** and Jianying Zhou, "Anomaly Detection in Industrial Control Systems using Logical Analysis of Data" in *Computer & Security* 2020.
- [6] **Sridhar Adep**, Luis Garcia, Ferdinand Brasser, Michael Rodler, Lucas Davi, Ahmad Reza Sadeghi, and Saman Zonouz, "Control Behavior Integrity for Distributed Cyber-Physical Systems" to appear in ICCPS-2020.
- [7] Nianyu Li, **Sridhar Adep**, Eunsuk Kang and David Garlan, "Explanations for Human-on-the-loop: A Probabilistic Model Checking Approach", to appear in *SEAMS@ICSE* 2020.
- [8] Umer, Muhammad Azmi, Aditya Mathur, Khurum Nazir Junejo, and **Sridhar Adep**. "Generating Invariants using Design and Data-centric Approaches for Distributed Attack Detection." *International Journal of Critical Infrastructure Protection* (2020): 100341.
- [9] **Sridhar Adep**, Eunsuk Kang, Aditya Mathur, " Challenges in Secure Engineering of Critical Infrastructure systems." *Automated Software Engineering Workshops(ASEW)*, 2019.
- [10] Chen, Yuqi, Christopher M. Poskitt, Jun Sun, **Sridhar Adep**, and Fan Zhang. "Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences." *Automated Software Engineering (ASE)*, 2019.
- [11] **Sridhar Adep**, Nandha Kumar Kandhasamy and Aditya Mathur "Investigation of Power Supply Interruption Attacks on Smart Grid" in *International Journal of Information Security*, 1-23, 2019.
- [12] Bytes Andrei, **Sridhar Adep**, and Jianying Zhou. "Towards Semantic Sensitive Feature Profiling of IoT Devices." *IEEE Internet of Things Journal* (2019).
- [13] **Sridhar Adep**, Aung Maw and Aditya Mathur "ICS-BlockOpS: Blockchain for Operational Data Security in Industrial Control System", *Special issue on Blockchain Technology and Applications in Pervasive and Mobile Computing* 2019.
- [14] **Sridhar Adep**, Nandha Kumar Kandhasamy and Aditya Mathur "EPIC: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security" in 4th Workshop On *The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS 2018)*.
- [15] **Sridhar Adep**, Aditya Mathur "Assessing the Effectiveness of Attack Detection at a Hackfest on Industrial Control Systems" in *IEEE Transactions on Sustainable Computing, Special Issue on Sustainable Cyber Forensics and Threat Intelligence* 2018.
- [16] **Sridhar Adep**, Aditya Mathur "Distributed Attack Detection in a Water Treatment Plant: Method and Case Study" in *IEEE Transactions on Dependable and Secure Computing* 2018.
- [17] Qin Lin, **Sridha Adep**, Sicco Verwer, and Aditya Mathur. "TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems." In Proceedings of the on *Asia Conference on Computer and Communications Security (ASIACCS)*, pp. 525-536. ACM, 2018.

- [18] Shrivastava Siddhant, **Sridhar Adep**, Aditya Mathur. "Design and assessment of an Orthogonal Defense Mechanism for a water treatment facility." *Robotics and Autonomous Systems*(2018).
- [19] Patlolla, Sai Sidharth, Bruce McMillin, Sridhar Adep, and Aditya Mathur. "An approach for formal analysis of the security of a water treatment testbed." In 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 115-124. IEEE, 2018.
- [20] Daniele Antonioli, Hamid Reza Ghaeini, **Sridhar Adep**, Martin Ochoa, and Nils Ole Tippenhauer. Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3. In Proceedings of the 2017 *Workshop on Cyber-Physical Systems Security and PrivaCy* (CPS '17).
- [21] Muhammad Azmi Umer, Aditya Mathur, Khurum Nazir Junejo, and **Sridhar Adep**. Integrating Design and Data Centric Approaches to Generate Invariants for Distributed Attack Detection. In Proceedings of the 2017 *Workshop on Cyber-Physical Systems Security and PrivaCy*(CPS '17).
- [22] **Sridhar Adep** and Aditya Mathur, "From Design to Invariants: Detecting Attacks on Cyber Physical Systems" *IEEE International Conference on Software Quality Reliability and Security*, 2017.
- [23] **Sridhar Adep**, Jay Prakash and Aditya Mathur, " WaterJam: An Experimental case study of Jamming Attacks on a Water Treatment System" *IEEE International Conference on Software Quality Reliability and Security*, 2017.
- [24] **Sridhar Adep**, Gyanendra Mishra and Aditya Mathur, " Access Controls in Water Distribution Networks: A Case Study " *IEEE International Conference on Software Quality Reliability and Security*, 2017.
- [25] Jonathan Goh, **Sridhar Adep**, Marcus Tan and Zi Shan Lee, " Anomaly Detection in Cyber Physical Systems using Recurrent Neural Networks", *Workshop on Security issues in Cyber Physical Systems (SecCPS) @ IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 2017, pp. 140-145. Best Paper Award.*
- [26] Giedre sabaliauskaite, **Sridhar Adep**, "Integrating Six-Step Model with Information Flow Diagrams for Comprehensive Analysis of Cyber-Physical System Safety and Security", *IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 2017.*
- [27] Koyena Pal, **Sridhar Adep**, Jonathan Goh, " Effectiveness of Association Rules Mining for Invariants Generation in Cyber-Physical Systems ", *IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 2017, pp. 124-127. Best Student Paper Award.*
- [28] **Sridhar Adep**, Jonathan Goh, Khurum Nazir Junejo, Aditya Mathur, "Secure Water Treatment (SWaT) Dataset," *the 11th International Conference on Critical Information Infrastructures Security 2016. Finalist Award for CIPRNET Young Critis Award CYCA (by European Union)*
- [29] **Sridhar Adep**, Giedre sabaliauskaite, Aditya Mathur, "A Six-Step Model for Safety and Security Analysis of Cyber-Physical Systems," *the 11th International Conference on Critical Information Infrastructures Security 2016.*
- [30] **Sridhar Adep**, Aditya Mathur, "Generalized attacker and attack models for Cyber Physical Systems," *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, 2016, pp. 283-292.*
- [31] **Sridhar Adep**, Aditya Mathur, "Using Process Invariants to Detect Cyber Attacks on a Water Treatment System," *31st International Conference on ICT Systems Security and Privacy Protection, (IFIP SEC), Belgium, 2016, pp 91-104*
- [32] Chuadhry Mujeeb Ahmed, **Sridhar Adep**, Aditya Mathur. "Limitations of State Estimation Based Cyber Attack Detection Schemes in Industrial Control Systems," *Smart City Security and Privacy Workshop (SCSP-W), Vienna, 2016, pp. 1-5.*
- [33] **Sridhar Adep**, Siddhant Shrivastava and Aditya Mathur " Argus: An Orthogonal Defense Framework to Protect Public Infrastructure against Cyber-Physical Attacks," in *IEEE Internet Computing, vol. 20, no. 5, pp. 38-45, Sept.-Oct. 2016.*
- [34] Eunsuk Kang, **Sridhar Adep**, Daniel Jackson and Aditya Mathur, "Model-Based Security Analysis of a Water Treatment System," *2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Pages 22-28, @ ICSE 2016.*
- [35] **Sridhar Adep**, Aditya Mathur, "Distributed Detection of SingleStage Multipoint Cyber Attacks in a Water Treatment Plant," *11th ACM on Asia Conference on Computer and Communications Security (ASIACCS 2016), Xi'an, China, 2016 Pages 449-460.*
- [36] **Sridhar Adep**, Aditya Mathur, "Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study," *2nd Asia Pacific conference on Complex Systems Design & management(CDSMAAsia) February 24-26-2016.*
- [37] **Sridhar Adep**, Aditya Mathur, "Detecting Multi-Point Attacks in a Water Treatment System Using Intermittent Control Actions," *Proceedings of Singapore Cyber Security Conference(SG-CRC), Volume 14, pp: 59 to 74, 2016.*
- [38] **Sridhar Adep**, Aditya Mathur, "An Investigation into the Response of a WaterTreatment System to Cyber Attacks," *The 17th IEEE International Symposium on High Assurance Systems Engineering (HASE2016).*

- [39] **Sridhar Adepu**, Aditya Mathur, Jagadeesh Gunda, Sasa Djokic, "Agent Based Framework for Simulating Cyber Physical Systems," Proceedings of *The 15th International Conference on Algorithms and Architectures for Parallel Processing ICA3PP* China, Nov 18-20, 2015, pp 785-798.

Patents

- [1] WATER-DEFENSE: A Method to Detect Multi-Point Cyber Attacks On Water Treatment Systems, U.S. Application No. 62/314,604
- [2] ARGUS: An orthogonal defense framework to protect public infrastructure against cyber physical attacks, US Application No. 10201607439T.
- [3] Association rule mining for invariants generation and attack detection in industrial control systems, 2017 (TD)
- [4] ICS:BlockOpS: Technolgy for Tamper Proofing Operational Plant Data in an Industrial Control System, 2018 (TD)
- [5] Ph UNDO: A Method for the Safe Operation of Critical Infrastructure Under Cyber Attacks, 2019 (TD).

SOFTWARE SKILLS *Languages:* Python, C, C++, Java, Matlab
 Web Technologies: HTML5, CSS
 Automation languages: Laddar logic, structure text

- PRESENTATIONS
- Invited talk on "*Attack Detection and Avoidance in Cyber Physical Systems*" at Missouri University of Science and Technology, Rolla, Missouri, September 2019.
 - Training to govt agencies on *attack modeling, design, implement and detection of industrial control systems*, 2017, 2018.
 - Invited talk on "*attacks and detection mechanisms in industrial control systems*" at National University of Singapore (NUS), August 2016.
 - Presented a poster on "*Attacker models for cyber physical systems*," in *Singapore cyber security conference SGCRC 2016*.
 - Presented a poster on "*Response of a cyber physical systems to cyber attacks: a case study*," in *Govware Singapore*, 2015.
 - Presented a Demo on "*How cyber attacks effects the Physical process in a water Treatment system*," *Secure Cyber Physical Systems Week, SUTD Singapore, 2015*.

REVIEWER

IEEE Sensors Journal (2020 to Present)
ACM, Transactions on Cyber-Physical Systems (2020 to Present)
IEEE Transactions on Information Forensics and Security (2019 to Present)
Elsevier, Future Generation Computing Systems (2019 to Present)
IEEE Transactions on Cybernetics (2019 to Present)
Springer, International Journal of Information Security (2019 to Present)
IEEE Access, (2019 to Present)
IEEE Transactions on Dependable and Secure Computing, (2019 to Present)
Elsevier, Journal of Information Security and Applications (2019 to Present)
IEEE Transactions on Industrial Informatics (2019 to Present)
IEEE IoT journal (2018 to Present)
IEEE Transactions on sustainable computing (2018 to Present)
Elsevier, International journal of critical infrastructure protection (2018 to Present)
Elsevier, Computers & Security (From 2017 to Present)

CO-REVIEWER CPSS 2020; ACNS 2019, 2020; AsiaCCS 2018,2019, 2020; ESORICS 2018,2019;
 SBES 2017; HASE 2017; COMPSAC 2016; CPS-SPC 2016,2018,2019; SG-CRC 2016.

EXTRA-CURRICULAR
ACTIVITIES

- *Local organising chair* for International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS), 2019 (Colombia), 2020 (Italy).
- *Local organising chair* for International Workshop on Security issues in Cyber Physical Systems (Sec-CPS) 2017(Singapore), 2019 (Hangzhou, China).
- Volunteered to help the organisers in 18th IEEE International Symposium on High Assurance System Engineering (HASE) 2017 (Singapore).
- Member of the researchers technical committee in SCy - Phy week 2015, 2016.
- Volunteered in Singapore Cyber Security R & D Conference (SG-CRC) 2016.
- Organised an event 'Project Exhibition' in Vignan University, 2013.
- Worked as a student Hostel Secretary, at Kakatiya University in 2010.
- Runner up in the zonal level basketball tournament, Khammam, Andhra Pradesh, 2009.
- Second position in 800 m running competition at university level sports meet, 2009.

REFERENCES

- Prof. Aditya P Mathur
Emeritus Professor
Computer Science, Purdue University
Center Director
iTrust Centre for research in Cyber Security
Singapore University of Technology and Design
Singapore 487372
Ph.: +65 9139 4552
email: aditya_mathur@sutd.edu.sg
- Prof. Jianying Zhou
Professor
Information Systems Technology and Design
Co-Center Director
iTrust Centre for research in Cyber Security
Singapore University of Technology and Design
Singapore, 487372
Ph.: +65 6499 8899
email:jianying_zhou@sutd.edu.sg
- Prof. Eunsuk Kang
Assistant Professor
Institute for Software Research
School of Computer Science
Canregie Mellon University
Ph.: +1(412) 268-3761
email: eskang@cs.cmu.edu