Sridhar Adepu, Ph.D.

Associate Professor in Cyber Security

CONTACT INFO

Office - 420, Computational Foundry, Bay Campus
Swansea, SA1 8EN, United Kingdom

Mobile: (+44)-7876756542
sridhar.adepu@swansea.ac.uk

AREAS OF INTEREST

Cyber-Physical Systems Security, Cyber-Physical AI Resilience & Resilience by Design for Critical Infrastructure

EDUCATION

Singapore University of Technology and Design, Singapore
PhD, Information Systems Technology and Design, 2016 to 2020

National Institute of Technology Rourkela, India
M.Tech., Computer Science and Engineering, 2011 to 2013

AWARDS

- **Best Paper** award in the 19th ACM ASIACCS2024.
- Awarded **NCSC RITICS Fellowship** 2023-2024.
- University of Bristol Research Fellowship 2023.
- Awarded the **CIPRNET Young CRITIS Award CYCA** in 2021.
- 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.

RESEARCH GRANT FUNDING

1) **Co-Investigator, EPSRC Securing Convergent Ultra-large Scale Infrastructures (SCULI), 2024-29, (£6,780,954):** I was co-leading one of the work package out of four work packages. This Programme grant is in collaboration with Oxford and Lancaster. **Airbus**, **British Telecom**, Vodafone, HP and **NCSC** are partners in this work. The project addresses the security of ultra-large-scale infrastructures, such as smart cities and Industry 4.0, by shifting the focus from traditional "security-by-design" to securing systems that may already be compromised. It integrates interdisciplinary expertise in cyber security, human-computer interaction, and threat analytics to provide predictable security assurances within highly complex and interconnected global environments. *This is a programme grant similar to the National Satellites of Excellence (NSoE) in Singapore, a highly competitive funding stream in the UK, (the success rate is ≈ 3).*

*Impact:*The project transforms national security by shifting the focus to securing compromised systems within ultra-large-scale infrastructures like smart cities and the aerospace sector. By translating **interdisciplinary research** into industry-validated techniques with partners, it provides a scalable blueprint for Smart Nation resilience and the commercialisation of trusted, global digital frameworks.

2) **Co-Principal Investigator EPSRC Supergen Energy Networks Impact hub 2023 , 2023 - 2028, (£5,334,575):** I am **leading the cyber security** research in the hub. We have more than 35 partners from industry, academia, regulators and government institutions. Department for the Economy (NI), Dept for energy security & net zero, Jacobs UK Limited, National Grid, **Ofgem**, **Siemens**, **Toshiba**, RITICS, **Wales & West Utilities** and **Northern Powergrid** are some of the partners in the hub. Please have a look at the link for details. *Highly competitive funding and only one hub funded in the entire UK, (the success rate is ≈ 3).*

*Impact:*This hub advances Smart Nation and Green Plan 2030 by securing the cyber-physical interface of net-zero energy networks. I drive the *translation* of risk and resilience to industry partners. This addresses national security by safeguarding energy networks, informing strategic policies for DSIT and DESNZ. A key measurable result includes *supporting new Ofgem policies to secure critical energy systems against systemic disruption*. The project strengthens human capital by prioritising Early Career Researcher (ECR) growth and participation in high-level industrial workshops. These efforts facilitate the sustainable adoption of green technologies and accelerate commercialisation, providing a validated blueprint for secure, high-value energy infrastructure. Extension to this project reinforces Singapore's status as a resilient, innovation-led global hub.

3) **Co-Principal Investigator EPSRC/DSTL RESICS:Resilience and Safety to attacks in ICS and CPS, (£1,093,750), 2023 - 2026:** Funded by DSTL UK for 3 years together with Imperial College London. I am leading PI from Bristol/Swansea. **Adelard**, Siemens, Airbus, **Thales** and **Carnegie Mellon University, USA** are partners. This project focuses on combination of data-driven and model-driven approaches. *Highly competitive funding and only three projects funded throughout the UK, the success rate is ≈ 5%.*

*Impact:*Advances national security by pioneering **safety and security** integrations in Industrial Control Systems. The project embeds **resilience-by-design** into critical infrastructure, ensuring the sustainable adoption of automated technologies. It translates research into industry-validated tools, strengthening human capital through global knowledge exchange. An extension of this project in Singapore provides a scalable pathway for commercialisation of safety and

security integrated solutions to resilience. This reinforces Singapore's status as a resilient, innovation-led global hub through measurable shifts in policy and practice.

4) **Principal Investigator, EPSRC Security Assurance of Semiconductor Manufacturing (SASM), 2025 - 2026, £92,000:** I lead the USA-UK collaborative project together with **SEMI-USA** on supply chain security of semiconductor manufacturing. **Techworks UK** and **Bavarian Chip Alliance** are local partners to realise the workshops to validate the outcome of the programme. *Highly competitive funding and industry impactful project, (the success rate is ≈ 7).*

Impact: This project has established a global community for semiconductor supply chain security, unifying international partners like S*EMI-USA, the Bavarian Chips Alliance, Applied Materials, ASML, Tokyo Electronics and NCSC RITICS*. Through workshops engaged 32 diverse organisations in semiconductor manufacturing,ensuring the framework is globally applicable and cost-effective. The project significantly reduces security compliance costs and questionnaire fatigue for suppliers. This collaborative project directly enhances the current practices in global semiconductor manufacturing within supply chain cyber security auditing. I am planning to extend this project in SUTD, which aligns with *Singapore's Research, innovation, and Enterprise (RIE) 2030 plan.*

5) **Principal Investigator, NCSC RITICS Fellowship, 2023 - 2024, £87000:** National Cyber Security Centre (NCSC) Research Institute in Trustworthy Inter-connected Cyber physical Systems (RITICS) Fellowship. This fellowship represents **thought leadership** in the Digital Twins Security in the UK. *Only two fellowships were awarded across the UK, making it a highly competitive achievement, (the success rate is ≈ 3).*

Impact: This project has shaped national policy by providing critical insights to government agencies and policy makers. A key outcome is the NCSC blog post on Digital Twins: secure design and development, establishing foundational security guidance for the sector. The work has catalysed national initiatives for Critical National Infrastructure (CNI), notably the Transit Hub initiative, which employs *50 million* digital twins to enhance sustainable transportation. By integrating security-by-design into policy and practice, the fellowship strengthens research infrastructure and human capital, ensuring the safe, sustainable adoption of Smart Nation technologies while addressing vital national security needs through global thought leadership.

6) **Principal Investigator, Innovate UK Knowledge Transfer Project (KTP) together with Synoptix 2023-2026, (£295,580.08):** This work focuses on applied AI to build a model (digital twin) which is used in anomaly detection caused by cyber-attacks. *Highly competitive and industry impactful project.*

*Impact:*The project focused on AI-driven cyber attack detection in water systems. This 27-month initiative has been a catalyst for growth, enabling Synoptix to launch its own dedicated cyber security group and expand its staff to 7 employees in cyber security. The output of the project is in TRL 7 and 8. Beyond organizational, business and commercial growth, the project has achieved significant academic and practical impact, with findings published in two research articles and presented at high-profile venues such as NCSC RITICS and BSides conferences.
Building on the success of this project, the Synoptix team is diversifying its expertise by targeting the maritime cyber security sector where Synoptix contributing 50% in the 2 million project (remaining 50% contrinuted by UKRI-EPSRC). This ongoing expansion reflects a successful bridge between academic research and industrial innovation to broader commercial and maritime autonomous platforms resilience.

7) **Outside UK:** I am Co-I researcher in *Automated Incident Response and Recovery in ICS* project in iTrust, SUTD under National Research Foundation, Singapore 325520 SGD (≈ £175,555). I am also a Co-I researcher in *Systematic Attack Generation for Industrial Control Systems* project in CyLab, CMU (≈ £76,000). I was also involved in Singapore-UK Cyber Security grant call in 2015 and our group received successful funding together with Imperial College London (≈ £280,000 Singapore share).

Research and Teaching Experience

Associate Professor in Cyber Security at Swansea University (February 2025 - Present)

Research Associates:

1. Dr. Sarad Vnugopalan, working on KTP with Synoptix.
2. Dr. Dipojjwal Ray, working on Safety and Security integration on RESICS project.

UG and MSc Supervision: Supervising 7 students every year for their thesis in cyber security.

Teaching: 1. IT-Security, Forensics & Cryptography, 2. Security Vulnerabilities and Penetration Testing (MSc)

Assistant Professor in Cyber Security at University of Bristol (September 2021 - February 2025)

Research Associates:

1. Dr. Sarad Vnugopalan, working on KTP with Synoptix.
2. Dr. Dipojjwal Ray, working on Safety and Security integration on RESICS project.
3. Kushagra Dixit, working on side channels in Industrail Systems.

PhD Co-Supervision:

1. Feras Shahbi on "Forensics in Industrial Control Systems"
2. Manolis Samanis on "Adaptive Security for Critical Infrastructure"

UG and MSc Supervision: Supervised 9 students every year for their thesis in cyber security.

Teaching:

1. Computer Systems (Introduction to Operating Systems and Security) (UG Module)

2. Resilient Socio-technical Infrastructures (PhD CDT module)
3. Security of Industrial Control Systems (MSc module)
4. IoT and IIoT Security (MSc Module)

Postdoctoral Researcher at ADSC, UIUC (May 2021 - August 2021)
Project: Attack-Resilient AI-Empowered Autonomous Cyber-Physical Systems.
Collaborative project between NTU and ADSC.

Visiting PhD student at Computer Science, Carnegie Mellon University, USA (July 2019 to Aug 2020)
Advisors: Prof. Eunsuk Kang and Prof. David Garlan
Project 1: Applying formal methods to Cyber Physical Systems security.
Project 2: Explainability of Autonomous Systems.

Teaching Assistant in Information Systems Technology and Design@SUTD (2017 to 2020)
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.

Research Assistant at iTrust, Centre for Research in Cyber Security, SUTD (Feb 2015 - Aug 2016)
Supervisor: Prof. Aditya P. Mathur, Involved in CYPRO and ASPIRE projects.
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, working with various government agencies to develop critical infrastructure protection.

Lecturer at Vignan University, India (June, 2013 - September, 2014)
Courses: Cyber Security, Data Structures and Software Engineering.
Thesis Mentored: Six Undergraduate and One Masters dissertation Projects.
Additional Responsibilities: Conducting laboratories, organizing workshops and seminars.

Teaching Assistant at National Institute of Technology, Rourkela, India (July 2011 - June 2013)
Courses: Data Structures, Algorithms, and Computer Programming in C language.

STARTUPS EXPERIENCE

Founder and Chief Scientist at ILLUSIONIQ Limited (January 2024 - Present) (70% FTE)
*Mission:*Architected security startup protecting CPS through AI-enabled cyber deception technology.
*Technology Translation & Product Development:*Led the transition of academic research into a commercial platform. Directed the development of PLC/SCADA decoys and OT-IT integrations, incorporating MITRE ATT&CK mapping and automated threat identification.
Fundraising & Strategic Investment: Won competitive investment funding (£500,000) by demonstrating high-fidelity detection and deception capabilities. Spearheaded discussions with institutional investors and government bodies to secure growth capital. Received UKRI-Innovate UK funding £50,000 to develop the scope of the project.
Business Development & Client Relations: Orchestrated strategic discussions with Critical Infrastructure organisations (energy, water, manufacturing). Defined the company's go to market strategy, positioning ILLUSIONIQ as a leader in proactive, security-by-design solutions. Successfully on-board businesses and generated revenue.
Leadership & Team Management: Built and managed a multi-disciplinary team of 10, including security, AI engineers and researchers. Cultivated a culture that balances research excellence with commercial agility.
Industry Influence: Served as a primary spokesperson at major events like the Utility Week Future Networks Conference, Bristol Tech Festival and London Tech Festival leveraging 12 years of CNI expertise.
Thought Leadership: Ensured product alignment with global security standards through active participation in international conference review boards and academic collaborations.
ILLUSIONIQ revolutionise cybersecurity for Critical Infrastructure by delivering cutting-edge deception platforms that anticipate and neutralise emerging threats.

Head of Research at Reperion(now Cequra) (June 2022 - December 2023) (40% FTE)
*Mission:*Spearheaded R&D to advance security products for mobile industrial assets from conceptual research to TRL 8 and 9 (fully commercialized or operationally deployed).
*Technical Product Engineering:*Guided the development of production-ready solutions focusing on Position Integrity (GNSS/navigation security), IT/OT Network Integrity, and Digital Asset Integrity for maritime and land assets. Implemented secure data exchange protocols for resilient communication.
*Detection & Triage:*Engineered autonomous detection systems to monitor and respond to converged cyber-physical threats across sea, land, and air platforms.
*Team Leadership:*Managed a multidisciplinary team of 7, synchronising deep-tech research with agile software development to ensure rapid deployment of mission-critical security features.
*Commercial Transition:*Aligned technical milestones with the company's strategy, delivering validated security prototypes for sovereign and industrial clients.

Reperion is a Singapore-headquartered with a global delivery capability to protect mobile assets across sea, land, and air from cyber-threats and cyber-attacks. Later, Reperion changed to Cequra and rebranding.

PATENTS

[1] WATER-DEFENSE: A Method to Detect Multi-Point Cyber Attacks On Water Treatment Systems, U.S. patent.
[2] ARGUS: An orthogonal defense framework to protect public infrastructure against cyber physical attacks, U.S. patent.
[3] ICS:BlockOpS: Technolgy for Tamper Proofing Operational Plant Data in an Industrial Control System, 2018 (U.S.).

PUBLICATIONS

[1] Dipojjwal Ray, Luca Castiglione, **Sridhar Adepu** and Emil Lupu. "CRASIS: Continuous Risk Assessment for Security Informed Safety" (In preparation for submission NDSS 2027)
[2] Venugopalan Sarad, and **Sridhar Adepu**. "GiBy: A Giant-Step Baby-Step Classifier For Anomaly Detection In Industrial Control Systems." arXiv preprint arXiv:2504.20906 (2025). (under review)
[3] **Sridhar Adepu**, Laiz Souto, Philip C. Taylor. "ILLUSIONIQ Cyber Deception in Energy Networks" 2025.
[4] **Sridhar Adepu**, Mark Goh. "ILLUSIONIQ Case Study - Critical Infrastructure Security Showdown (CISS)" 2025.
[5] Maganti Praneeta, Rajib Ranjan Maiti, and **Sridhar Adepu.** "Identifying CIP-centric Attacks in CPS." In 2025 *17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, pp. 867-870. IEEE.
[6] Ruizhe Wang, Sarad Venugopalan and **Sridhar Adepu**. "Safety Analysis for Cyber-Physical Systems Under Cyber Attacks Using Digital Twin", In Proceedings of the *IEEE International Conference on Cyber Security and Resilience (CSR)*, London, 2024.
[7] Mathuros, Kornkamon, Sarad Venugopalan, and **Sridhar Adepu**. "WaXAI: Explainable Anomaly Detection in Industrial Control Systems and Water Systems." In Proceedings of the 10th *ACM Cyber-Physical System Security Workshop*, pp. 3-15. 2024. Awarded Best Paper Award
[8] Li, Nianyu, Mingyue Zhang, Jialong Li, **Sridhar Adepu**, Eunsuk Kang, and Zhi Jin. "A Game-Theoretical Self-Adaptation Framework for Securing Software-Intensive Systems." *ACM Transactions on Autonomous and Adaptive Systems* 19, no. 2 (2024): 1-49.
[9] Alfageh, Alyah, Sridhar Adepu, and Charalambos Konstantinou. "Water Risk-Proofed: Risk Assessment in Water Desalination." In Proceedings of the 5th *Workshop on CPS&IoT Security and Privacy*, pp. 11-23. 2023.
[10] Shahbi, Feras, Joseph Gardiner, **Sridhar Adepu**, and Awais Rashid. "A Digital Forensic Taxonomy For Programmable Logic Controller Data Artefacts." In 2023 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* pp. 320-328. IEEE, 2023.
[11] Cai, Tianyang, Tao Jia, **Sridhar Adepu**, Yuqi Li, and Zheng Yang. "ADAM: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system." IEEE Transactions on Industrial Informatics 19, no. 6 (2023): 7802-7813.
[12] Jin, Chenglu, Zheng Yang, Tao Xiang, **Sridhar Adepu**, and Jianying Zhou. "HMACCE: establishing authenticated and confidential channel from historical data for industrial internet of things." *IEEE Transactions on Information Forensics and Security* 18 (2023): 1080-1094.
[13] Ahalawat, Anchal, **Sridhar Adepu**, and Joseph Gardiner. "Security threats in electric vehicle charging." In 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pp. 399-404. IEEE, 2022.
[14] Zhu, Yuqing, **Sridhar Adepu**, Kushagra Dixit, Ying Yang, and Xin Lou. "Adversarial attacks and mitigations on scene segmentation of autonomous vehicles." In *European Symposium on Research in Computer Security*, pp. 46-66. 2022.
[15] **Sridhar Adepu**, Nianyu Li, Eunsuk Kang, and David Garlan. "Modeling and analysis of explanation for secure industrial control systems." ACM Transactions on Autonomous and Adaptive Systems 17, no. 3-4 (2022): 1-26.
[16] **Sridhar Adepu**, Nianyu Li, Eunsuk Kang, and David Garlan. "Modeling and Analysis of Explanation for Secure Industrial Control Systems." *ACM Transactions on Autonomous and Adaptive Systems*. (2022).
[17] Balaji, Madhumitha, Siddhant Shrivastava, **Sridhar Adepu**, and Aditya Mathur. "Super Detector: An Ensemble Approach for Anomaly Detection in Industrial Control Systems." In *International Conference on Critical Information Infrastructures Security*, pp. 24-43. 2021. Awarded the Critical Infrastructures Preparedness and Resilience Research Network (CIPRNET) Young CRITIS Award
[18] Yang Zheng, **Sridhar Adepu**, and Jianying Zhou. "Opportunities and Challenges in Securing Critical Infrastructures Through Cryptography." *IEEE Security & Privacy* 19.5 (2021): 57-65.
[19] **Sridhar Adepu**, Mathur, Aditya. "SafeCI: Avoiding process anomalies in critical infrastructure." *International Journal of Critical Infrastructure Protection* 34 (2021): 100435.
[20] Palleti Venkata Reddy, **Sridhar Adepu**, Vishrut Kumar Mishra, and Aditya Mathur. "Cascading effects of cyber-attacks on interconnected critical infrastructure." *Cybersecurity* 4, no. 1 (2021): 1-19.
[21] Josephlal, Edwin Franco Myloth, **Sridhar Adepu**, Zheng Yang, and Jianying Zhou. "Enabling isolation and recovery in PLC redundancy framework of metro train systems." *International Journal of Information Security (2021)*: 1-13.
[22] **Sridhar Adepu**, 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.
[23] Tanmoy Kanti Das, **Sridhar Adepu** and Jianying Zhou, "Anomaly Detection in Industrial Control Systems using Logical Analysis of Data" in *Computer &Security* 2020.
[24] **Sridhar Adepu**, 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.
[25] Nianyu Li, **Sridhar Adepu**, Eunsuk Kang and David Garlan, "Explanations for Human-on-the-loop: A Probabilistic Model Checking Approach", to appear in *SEAMS@ICSE* 2020.
[26] **Sridhar Adepu**, Nandha Kumar Kandasamy, Jianying Zhou, and Aditya Mathur. "Attacks on smart grid: Power supply interruption and malicious power generation." International Journal of Information Security 19, no. 2 (2020): 189-211.
[27] Umer, Muhammad Azmi, Aditya Mathur, Khurum Nazir Junejo, and **Sridhar Adepu**. "Generating Invariants using Design and Data-centric Approaches for Distributed Attack Detection." *International Journal of Critical Infrastructure Protection* (2020): 100341.
[28] **Sridhar Adepu**, Eunsuk Kang, Aditya Mathur, " Challenges in Secure Engineering of Critical Infrastructure systems," *Automated Software Engineering Workshops(ASEW)*, 2019.

[29] Chen, Yuqi, Christopher M. Poskitt, Jun Sun, **Sridhar Adepu**, and Fan Zhang. "Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences." *Automated Software Engineering (ASE)*, 2019.

[30] Bytes Andrei, **Sridhar Adepu**, and Jianying Zhou. "Towards Semantic Sensitive Feature Profiling of IoT Devices." *IEEE Internet of Things Journal* (2019).

[31] **Sridhar Adepu**, 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*. Singapore National Blockchain Challenge Gold medal award and ASEAN ICT Gold medal award in research and development, 2018.

[32] **Sridhar Adepu**, 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)*.

[33] **Sridhar Adepu**, 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*.

[34] **Sridhar Adepu**, Aditya Mathur "Distributed Attack Detection in a Water Treatment Plant: Method and Case Study" in *IEEE Transactions on Dependable and Secure Computing* 2018.

[35] Qin Lin, **Sridha Adepu**, 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.

[36] Shrivastava Siddhant, **Sridhar Adepu**, Aditya Mathur. "Design and assessment of an Orthogonal Defense Mechanism for a water treatment facility." *Robotics and Autonomous Systems*(2018). Finalist in Techblazer award, *SG:TECH*, 2021. National level prestigious award

[37] Patlolla, Sai Sidharth, Bruce McMillin, Sridhar Adepu, 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.

[38] Daniele Antonioli, Hamid Reza Ghaeini, **Sridhar Adepu**, 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).

[39] Muhammad Azmi Umer, Aditya Mathur, Khurum Nazir Junejo, and **Sridhar Adepu**. 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).

[40] **Sridhar Adepu** and Aditya Mathur, "From Design to Invariants: Detecting Attacks on Cyber Physical Systems" *IEEE International Conference on Software Quality Reliability and Security*, 2017.

[41] **Sridhar Adepu**, Jay Prakash and Aditya Mathur, " WaterJam: An Experimental case study of Jamming Attacks on a Water Treatment System" *IEEE Intern. Conference on Software Quality Reliability and Security*, 2017.

[42] **Sridhar Adepu**, Gyanendra Mishra and Aditya Mathur, " Access Controls in Water Distribution Networks: A Case Study " *IEEE International Conference on Software Quality Reliability and Security*, 2017.

[43] Jonathan Goh, **Sridhar Adepu**, 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.

[44] Giedre sabaliauskaite, **Sridhar Adepu**, "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*.

[45] Koyena Pal, **Sridhar Adepu**, 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.

[46] **Sridhar Adepu**, Jonathan Goh, Khurum Nazir Junejo, Aditya Mathur, "A Dataset to Support Research in the Design of Secure Water Treatment Systems," *the 11th International Conference on Critical Information Infrastructures Security 2016*. Finalist Award for CIPRNET Young Critis Award CYCA (by European Union)

[47] **Sridhar Adepu**, 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*.

[48] **Sridhar Adepu**, 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*.

[49] **Sridhar Adepu**, 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*

[50] Chuadhry Mujeeb Ahmed, **Sridhar Adepu**, 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*.

[51] **Sridhar Adepu**, 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.*

[52] Eunsuk Kang, **Sridhar Adepu**, 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*.

[53] **Sridhar Adepu**, 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.*

[54] **Sridhar Adepu**, 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(CDSMAsia) February 24-26-2016*.

[55] **Sridhar Adepu**, 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.

[56] **Sridhar Adepu**, 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)*.

[57] **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.

SELECTED INVITED TALKS

- Invited talk at NCSC RISE Showcase, London 2026.
- Invited talk at NCSC RITICS Showcase, London 2026.
- Invited talk at CyberCon, Bristol Tech festival 2025.
- Invited talk at Utility Conference, 2025.
- Invited talk at NCSC RITICS annual conference Feb 2024, London.
- *Invited talk* at Cyber Security Education Research Conference Kuwait, **by Britsh Embassy**, 2023 and 2024.
- *Invited talk* at international workshop on "Data Mining and Machine Learning applied to CPS, 2022.
- *Invited talk* at University of Strathclyde, 2022
- *Invited talk* at UK Cyber Security **PhD Winter School** 2022.
- keynote delivered at World Intelligent Manufacturing Conference 2021
- *Invited talk* at Zhejiang University, November 2021
- *Invited talk* on "*Attack Detection and Avoidance in Cyber Physical Systems*" at Missouri University of Science and Technology, Rolla, Missouri, September 2019.

SELECTED PROFESSIONAL ACTIVITIES

Conference/Workshop Chair:

- **Programme Committee Chair** at International Workshop on Impact of IT/OT Convergence on the Resilience of Critical Infrastructures (IOCRCI) 2024 and 2025.
- **Programme Committee Chair** at 2024 IEEE CSR Workshop on Security, Privacy and Resilience of Critical Assets in Critical Infrastructure (SPARC), in London
- Organised National level event on Digital Twins for CNI security with NCSC/RITICS, Feb 2024 in London.
- **Publicity chair** at 19th International Conference on Security& Privacy in Communication Networks (Securecomm 2023), in Hong Kong.
- **Publicity chair** at AIoTS workshop at the 21st International Conference on Applied Cryptography and Network Security 2023, in Japan.
- **Publicity chair** at Security of Electric Vehicle Charging (SecEVC) workshop at 15th IEEE International Conference on Smart Grid Communications (SmartGridComm 2022), in Singapore
- **Guest Editor** in "Privacy-Enhancing Authentication and Computation for human CPS and IOT" *Security and Communication Networks Journal*, 2022
- **Programme Committee Chair** for the Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS) workshop at *ACNS2022*.
- **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 (SecCPS)* 2017(Singapore), 2019 (Hangzhou, China).
- Member of the researchers technical committee in SCy - Phy week 2015, 2016.

Conference/Journal Reviewer:

- Workshop on CPS & IoT Security and Privacy (CPSIoTSec) at ACM CCS 2022, 2023, 2024, 2025, 2026.
- The 19th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2024)
- International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS@ICSE 22, 23, 24)
- ACM SIGEnergy Workshop on Cybersecurity and Privacy of Energy Systems (EnergySP) 2024, 2025, 2026.
- Cyber Physical Systems Security @ASIACCS23
- 17th International Conference on Network and System Security 2023
- IEEE Security and Privacy (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 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)
- Elsevier, International journal of critical infrastructure protection (2018 to Present)
- Elsevier, Computers & Security (From 2017 to Present)