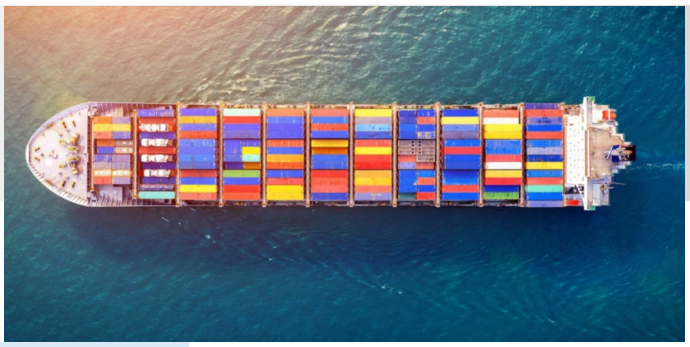
iTrust Times

A Quarterly Newsletter

Issue Highlights:

- iTrust Maritime Webinar *pg. 2*
- Guidelines on maritime cybersecurity *pg. 3*
- Remote access to testbeds *pg. 3*
- Visit by Wartsila *pg. 4*
- iTrust internship *pg. 4*
- Awards *pg. 6*



Jan—Mar 2022 | Volume 8 Issue 1

From Centre Director's Desk

Forging Ahead

Dear Reader:

Greetings from iTrust!

We are at the end of the first quarter of 2022 and iTrust is, as usual, buzzing with activities.

This is the first time the full 6-stage water treatment digital twin will be used during an international cyber exercise. The latest version of the 6-stage twin mimics all stages of the SWaT water treatment plant located in SUTD. The twin enables launch of attacks via the manipulation of network traffic across the PLCs and SCADA as well as directly by attacking specific devices such as valves and pumps. A new addition to the twin is a professional looking "OT Vision" designed, implemented, and integrated by one of our interns Derrick Lim with guidance from our Cyber Tech Lead Francisco Furtado. Two anomaly detectors are also integrated with the twin.

Research on Maritime security is moving at rapid speed in iTrust. Thanks to the research team led by Professor Jianying Zhou, guidelines for cyber-risk management in Shipboard Operational technology are now available for download. Professor Jianying and Mark Goh have begun search for physical space where the Maritime testbed will be located.

I am happy to announce that remote access to all our water and electric power testbeds is now available. Remote access, via VPN, will enable access to PLCs, RTUs, etc, making it easier for iTrust researchers to collaborate with international partners.

Members of iTrust continue to receive accolades. Dr Daniel Reijsbergen and Aung Maw won the first prize in the Enthusiast Track during the Singapore Blockchain Hackathon. Siddhant Shrivastava continued his "award winning" streak by clinching the Excellent in Service award at SUTD. Congratulations to the winners!

That is all for now. Happy reading and best wishes to all readers of iTrust Times for a productive and happy 2022!

Aditya Mathur
Centre Director, iTrust, SUTD
Director, National Satellite of Excellence DeST-SCI
Professor Emeritus, Computer Science, Purdue University

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

Research Focus

iTrust Maritime Webinar

Bearing fruit

iTrust ran its fourth webinar on maritime cybersecurity on 25 Feb 2022, in partnership with the Centre of Excellence in Maritime Safety (CEMS) at Singapore Polytechnic. The webinar is a **culmination of a year-long study led by iTrust Co-centre Director Prof Jianying Zhou on cyber risk management for shipboard OT (operational technology systems).** Prof Zhou's team presented the study's findings at three webinars over an 8-month period.

In his opening remarks, Mr Tan Cheng Peng, the Executive Director of the Singapore Maritime Institute (SMI), which funded the study, commended the team "for having done a great job in amalgamating the 'best practices' as a starting guideline for maritime authorities and ship owners in Singapore to better manage cyber risk of shipboard systems." On the concrete outcomes from the study, Mr Tan shared, "I am happy to note that the guidelines will also be **shared by MPA as an information paper in IMO's 105th session of the Maritime Safety Committee** under the agenda item 'Measures to enhance maritime security'. On top of this, the guidelines were used to **support the cyber category of the Singapore Registry of Ships (SRS) notations launch by MPA** in November last year. The "Cyber" notation is awarded to vessels that have adopted advanced cyber security measures to protect their key shipboard operational technology systems from cyber attacks."

Ms Priyanga Rajaram, the senior research assistant who was responsible for large swathes of the study and putting the guidelines together, presented the following key findings in the guidelines: the cyber risks in shipboard OT systems, the cyber risk assessment of the identified risks, the three security tiers that could be adopted to achieve cyber readiness and a sample checklist to (self) assess the cyber hygiene. The guidelines are available freely for download at iTrust's website: https://bit.ly/3ipaJCQ

Prof Zhou then shared his team's next **phase in maritime cyber research: a planned maritime testbed of shipboard OT systems for research, training, education and cyber exercises.** Next, Capt Ashwin Madhav Khandke (top right in Figure 1), a senior lecturer from SP, shared his extensive experience as a ship master on maritime cybersecurity, where an increase in the number of integrated systems onboard a ship led to an increase in the attack surfaces that a cyber attacker could exploit (Figure 3). As a response, Capt Khandke **espoused the concept of security by design,** in which he said, "The industry needs to establish meaningful standards to meet these (cyber) risks and then create strategies to meet those demands. (In addition), equipment manufacturers must take note of the (every-changing) threat landscape with a view to enhancing the reliability of the system."

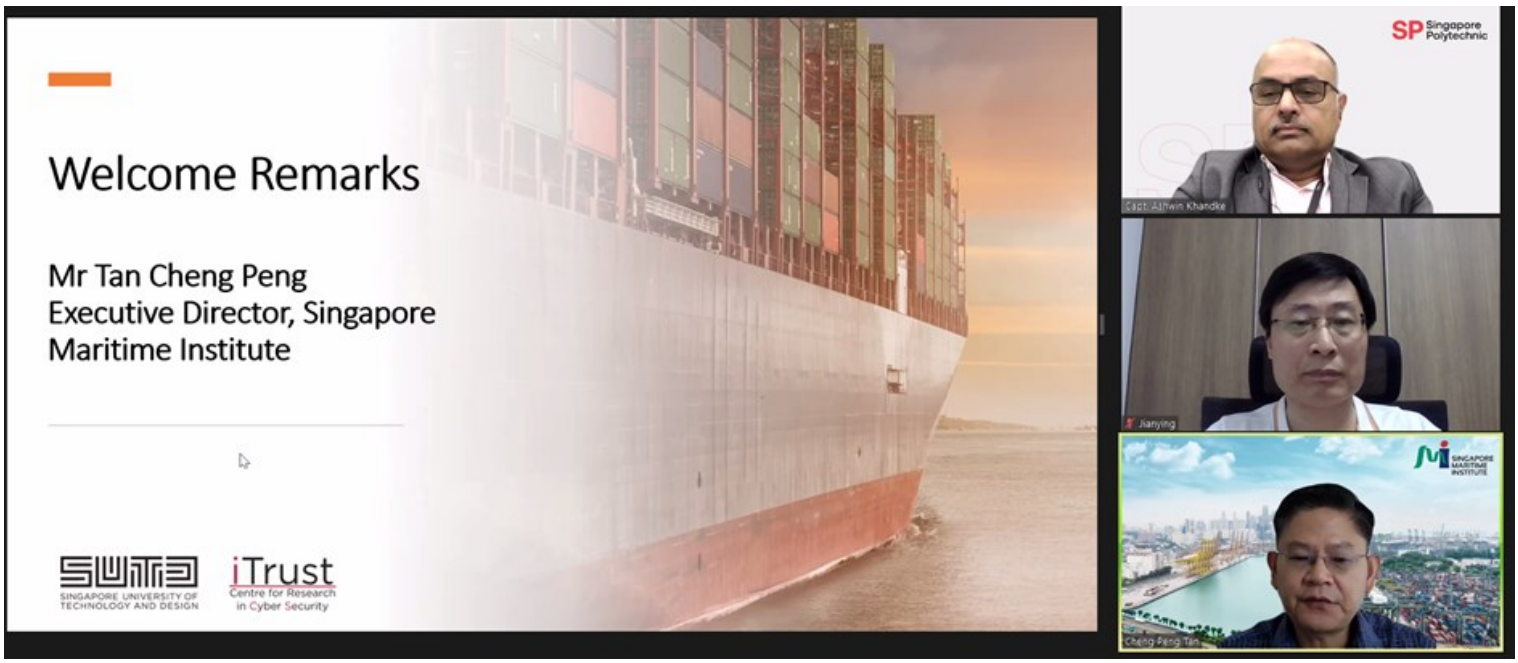


Figure 1: SMI Executive Director Mr Tan Cheng Peng (bottom right) giving his welcome remarks at the iTrust maritime cybersecurity webinar

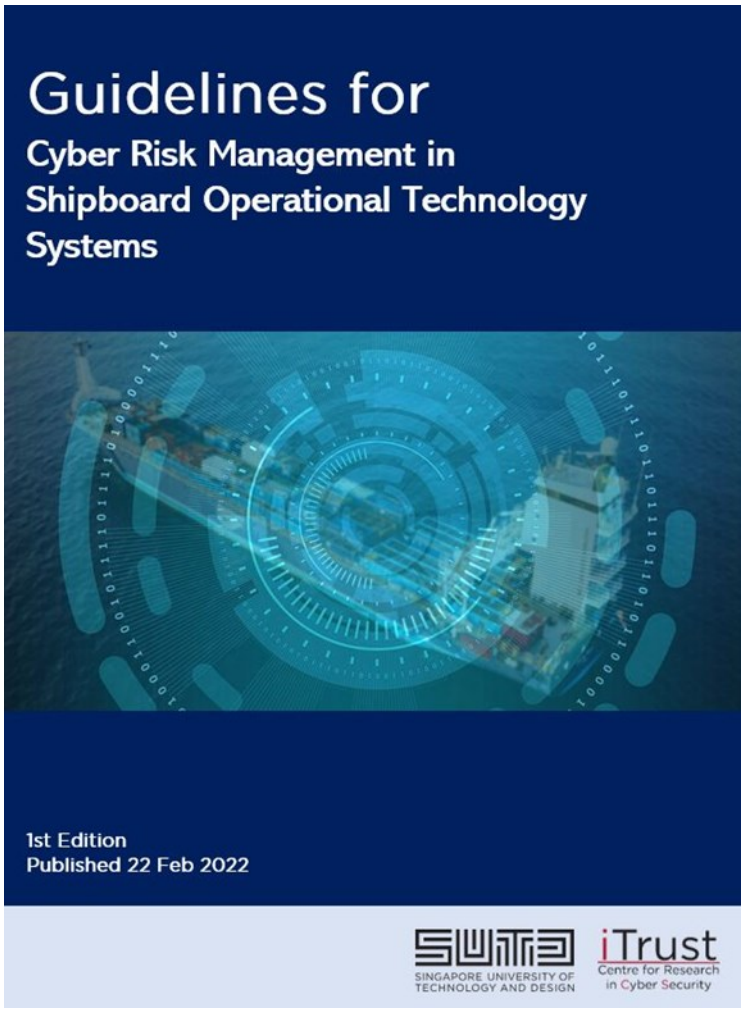


Figure 2: A copy of the guidelines is available for download

After a round of Q&A session, Mr Daniel Zhang, CEMS' Centre Director, then closed the webinar by drawing an analogy between cyber attacks and COVID infection, where increased connectivity/interactions inevitably leads to a high risk of attack/infection. In that, he believed that "getting prepared is very important," and doing so will help one face cyber incidents more readily.

iTrust wishes to thank the Singapore Maritime Institute (SMI) for funding the study, and the Maritime and Port Authority of Singapore (MPA) for its support. It also wishes to acknowledge the American Bureau of Shipping (ABS), KPMG, CEMS and the Singapore Shipping Association (SSA) for their valuable feedback on the guidelines.

Remote Access to iTrust Testbeds

Access just got easier

Remote access to iTrust testbeds (SWaT, WADI and EPIC) is available to all researchers, government organisations and industry during office hours (GMT +8). To facilitate the remote access, a VPN connection will be established to provide a tunnelled route into the testbeds' operational network. From there, remote users will be able to access Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human machine

Figure 3: With great(er) connectivity comes great(er) risks: Increased attack surfaces onboard ships

Interfaces (HMIs) and the infrastructure of the testbeds.

With this setup, users are no longer restricted by their geographical location and can enjoy the near-full experience of using the testbeds for their research. For now, usage of the testbeds via remote access is limited to office hours (GMT+8) and subject to rental charges. Please visit iTrust's website for details on the charges and how to secure a slot.

Figure 4: Remote access to world-class critical infrastructure testbeds is now possible

Visits

Navigating new domains

With iTrust now adding the maritime domain into its list of focus areas, it has been gaining traction and attention in the maritime industry. In this, iTrust Co-centre Director Prof Jianying Zhou has been busy interacting with various maritime companies and associations, from ship builders to equipment manufacturers and the Cybersecurity sub-committee in the Singapore Shipping Association. On 23 Feb, Prof Zhou hosted Mr Mark Milford, who is the Global Vice President for Cybersecurity at Wärtsilä, a Finnish equipment manufacturer of innovative technologies and lifecycle solutions for the marine and energy markets. He was introduced to the cyber capabilities and facilities at iTrust and was also excited at our plans to build a maritime testbed for shipboard OT cybersecurity research. Mr Milford was accompanied by Mr Chris Chung, Director of Digital Innovation & Strategic Projects, Mr Bhupesh Gandhi, Simulation Expert and Mr Juha Hollanti, Senior Rapid Prototyping Specialist – Rapid Innovation.

Figure 5 (left to right): Prof Zhou introducing SWaT to Mr Hollanti, Mr Milford and Mr Gandhi (photo credit: Mr Chris Chung)

Internship

Power Rangers

iTrust trains a new crop of interns in OT cybersecurity

OT Vision - Seeing is Believing

by Derrick Lim

Over the past three months at iTrust, I've had the opportunity to work with my mentor, Francisco Furtado, iTrust's Cyber Tech Lead, to explore solutions in visualising the plant that can bring benefits to various stakeholders of the plant (e.g. plant operators and engineers.) We created **OT Vision, a visualisation tool to provide a graphical illustration of the plant's status.** OT Vision uses visual elements like charts, graphs, and tables to provide an accessible way to understand the plant's status and patterns using data. The objective of OT Vision is to provide a centralised platform to holistically visualise Secure Water Treatment (SWaT), Water Distribution (WADI), and Electric Power and Intelligent Control (EPIC) testbeds.

OT Vision provides plant engineers with **greater situation awareness by visualising anomalies detected** from the various anomaly detectors and presenting them in a dashboard. Using data collected, OT Vision can help identify trends such as the rate at which water is rising in a tank, the pH level of the water, or even the difference between the actual and predicted values of the tank's water level.

OT Vision opens up numerous possibilities to monitor

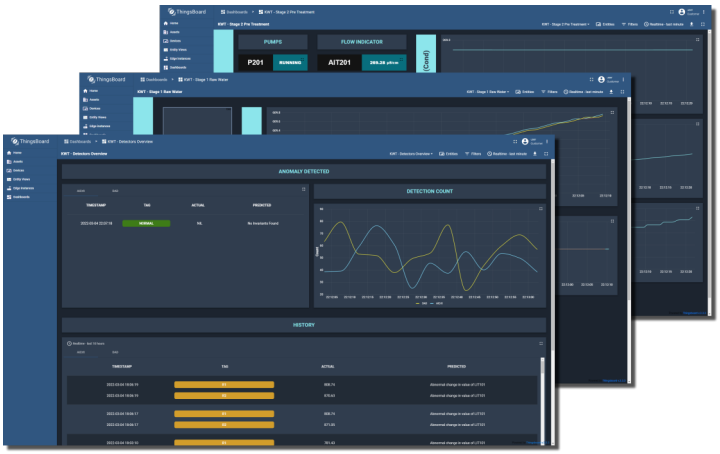


Figure 6: Various screenshots of OT Vision showing status of anomaly detectors (front) and plant behaviour (back)

and detect anomalies in the plant, hence creating another layer of security for the plant. I am proud of my achievement in iTrust and excited to see how OT Vision can play a part in protecting the security of our critical infrastructure.

PlantProtect and Correct

By Tiger Lim

Modern-day cyber-physical attacks on critical infrastructure (such as water plants) are unpredictable, dangerous and on the rise. These attacks can be stealthy, causing major damage to the plant before being discovered. Sophisticated attackers have also found ways to compromise IT systems in such plants. For example, after the attacker compromises the IT network, they are able to access the Level 1 network which holds the SCADA interface (Supervisory Control and Data Acquisition) along with all the PLCs (Programmable Logic Controllers) that control the plant. From there, the attacker can launch stealthy attacks, manipulating the integrity of the network packets. Hence, preventing attacks at both the IT and OT level of the plant is critical, as are the locations where the anomaly detectors are placed within the plant to ensure the integrity of the commands and communication.

In that regard, I am working on developing a **strengthened version of PlantProtect** that can detect preliminary checks at Level 0 and Level 1 of the network. To protect against such attacks, PlantProtect is placed at Level 1 of the plant to capture the overall plant situation by retrieving data communicating between the SCADA and PLCs. It also retrieves raw data from Level 0, between the RIO (Remote Input/ Output) and the PLC, converting digital values to current/voltages and vice versa. With those data, PlantProtect compares it to predicted values from other anomaly detectors that use machine learning/artificial intelligence to estimate the normal-state values. Finally, **PlantProtect corrects the values on both Levels before they reach the actuator or sensor.**

AICrit-IT: With Our Powers Combined

By Max Ong

I have been given the opportunity to work with Dr Gauthama Raman to develop AICrit-IT, **a multi-level Intrusion Detection System (IDS)** to safeguard the Secure Water Treatment (SWaT) and Water Distribution (WADI) testbeds.

Using a data-centric machine learning algorithm coupled with design knowledge of the plants (design-centric approach), AICrit-IT precisely learns **the normal spatiotemporal relationship among the set of highly correlated components** within the plants. It analyses every packet in the network and processes it through four sequential layers of validation. The first and second layers are to authenticate the packet's IP and MAC address against a list of whitelisted IP and MAC addresses. Thereafter, it reaches the third layer where the packet will be analysed based on a behavioural model created on the testbed's normal operating behaviour.

Upon successfully going through the three layers, the packet will undergo a **payload analysis layer.** At this stage, the packet's payload will be dissected and decoded to obtain certain values. These values will be compared against the predicted values from the existing AICrit-OT (operational technology). At any stage where the packet fails the layer's validation, an alert will be raised.

AICrit-IT as a multi-level detector will be an useful asset as it is capable of generating alerts given different attack scenarios.

Attack Desk: A Buffet of Attacks

By Aaron Peh

During the past three months in iTrust, I have been building on the good work done on the Attack Desk by previous researchers. The Attack Desk is a library **of about 20 attacks that researchers can use to launch attacks** on the Secure Water Treatment (SWAT) Water Distribution (WADI) testbeds and digital twin. This suite of attacks can be used to **test the robustness of anomaly detectors** with a view of improving them, as well as for users to view the **potential impact of those attacks on a critical infrastructure.**

My work involves creating a webpage interface for Attack Desk, so that users who are able to view the attack description, select the type of attacks and the attack surfaces on which they wish to launch the attacks. I have also **expanded the library with another 60 attacks.** Some of these attacks include damaging the physical plant, masking attacks, denial of service (DOS), poisoning the water supply and wastage/ flooding of water.

Together in Electric Attacks

By Valentino Tok & Kenneth Wang

We are assigned to the Electric Power and Intelligent Control (EPIC) testbed and develop viable attack scripts on power systems. This required deep diving into how the OT devices in EPIC co-relate and work with each other, and how they would respond to command inputs from the SCADA. We also developed an understanding of the PLC code, the relevant libraries used and the communication protocols used between SCADA and the OT devices.

With this, we were then able to develop attack scripts on the EPIC testbed. These scripts are capable of extracting data from the system, **as well as mimicking commands given as the SCADA device to gain control** over the entire testbed. An attacker can then disrupt any running services, for example, by opening the breakers and prevent power supply to consumers. The attacker can also constantly **toggle the breakers to switch them on and off,** resulting in their wear and tear. Another attack that we developed was a man-in-the-middle **(MITM) attack between the VSD and PLC.** Doing so gives the attacker control over the speed and status of the generator's motor, thereby preventing the generator from reaching the required speed to produce power and disrupting power supply.
Using the common industry communication protocol - IEC 61850 – we also developed an attack script to **control the load bank.** This allows the attacker to increase or decrease the amount of load and control other options available to the load bank, thereby forcing the plant to erroneously increase or decrease power to the loads.

Moving forward, we plan to **exploit the vulnerabilities of the SCADA** to gain access into the OT network and conduct post-exploitation actions like adding network routes, uploading and running executable and acquiring credentials. We also plan to automate the entire process in a single script.

Awards

iTrust in Stanford University's List of Top 2% Scientists

iTrust Centre Director Prof Aditya Mathur and Co-Centre Director Prof Jianying Zhou were among the 24 SUTD faculty members to enlisted into the global list of top 2% scientists in their respective fields of "Design of secure and safe critical infrastructure" and "Cyber security." Congratulations!

Blockchain Hackathon 2021

A team comprising Research Fellow Dr Daniel Reijsbergen and Research Assistant Aung Maw, won the first prize (Enthusiast Track) in the Singapore Blockchain Hackathon 2021. In their winning entry, PIEChain, they implemented an interoperability solution for existing blockchains, and demonstrated it with two applications: cross-chain auction and cross-chain flash loan.

The Singapore Blockchain Innovation Challenge is hosted by Singapore Blockchain Innovation Programme (SBIP) - a collaborative and nationwide technical

community, launched from a mandate to further strengthen Singapore's blockchain ecosystem. The competition invites participants to develop innovative protocols, frameworks, and use cases for blockchain interoperability. Well done!

Figure 7: Dr Daniel Reijsbergen (far left) and Aung Maw (centre) pose with their certificate of achievement and Asst Prof Dumitrel Loghin (NUS), one of the organisers of the hackathon.

SUTD Awards

Research Associate Siddhant Shrivastava was presented with the Excellence in Service to the Community award at the SUTD Awards ceremony on 25 Feb 2022. This award is given to an individual who has made an extraordinary, significant contribution to the betterment of society.

In receiving the award, the successful recipient has positively affected society by fostering long-term change to the public good, employed an innovative approach to their service; and emerged and is distinctive among peers as an individual whose service has produced extraordinary results. Congratulations, Siddhant!

Looking Ahead in 2022

Datasets? Yes, please

As we begin the year, we would like to share with our readers the reach and impact of iTrust's work. Through the good work our researchers have done and from the various activities that iTrust organises over the past six years, we have generated and collected a treasure trove of datasets from our critical infrastructure and IoT testbeds.

There have been **over 6,000 requests by researchers from more than 2,000 organisations—both academia and private organisations— hailing from 70 countries.** We are proud of this milestones and hope the datasets will be put to good use to better secure critical infrastructures around the world.

The datasets are available free of charge, upon request on our website, for anyone around the world to use for their research, study, experiments etc.

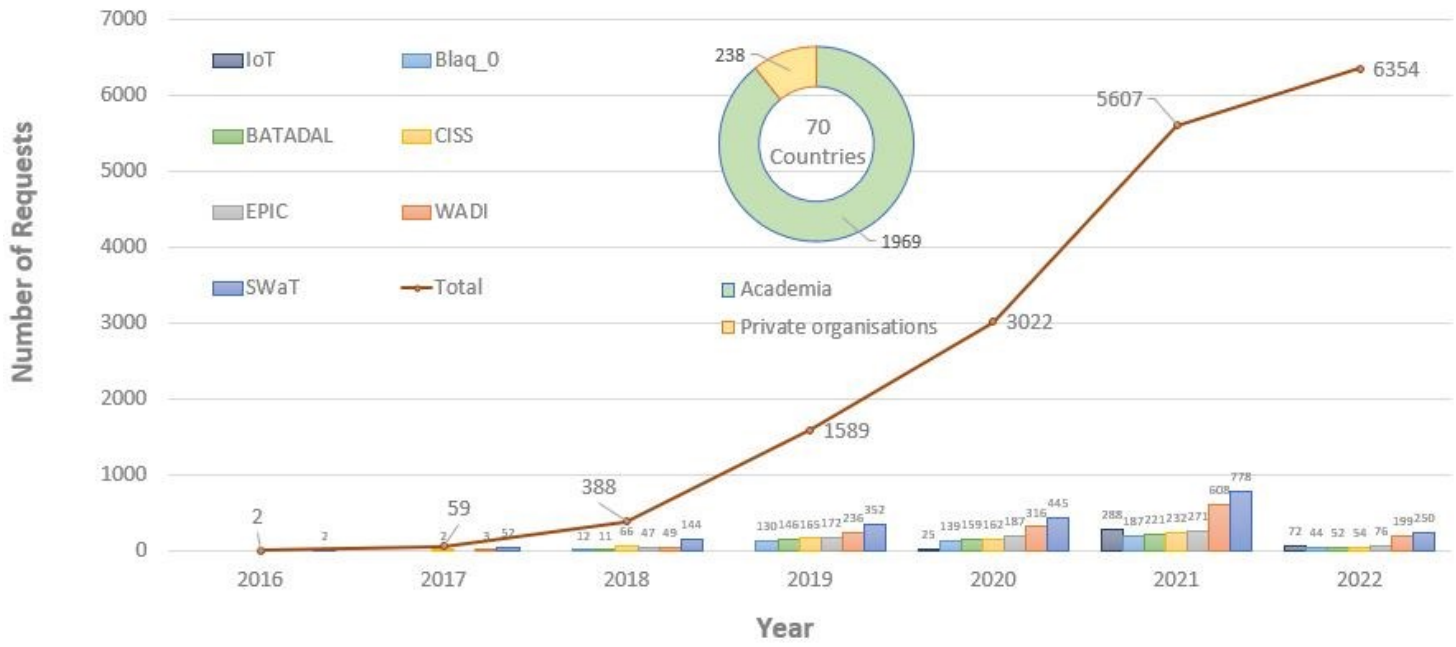


Figure 8: Dataset requests by the numbers

LinkedIn

iTrust is now on LinkedIn — connect with us! Feel free to reach out to us to explore research

collaborations, testbed usage and training and testing services. Email addresses end with the domain *@sutd.edu.sg*

Management

Prof. Aditya P MATHUR
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur

Prof. Jianying ZHOU
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
jianying_zhou

Francisco FURTADO
Cyber Tech Lead, iTrust
francisco_dos

Mark GOH
Associate Programme Director, iTrust
Editor, iTrust Times
mark_goh

iTrust Laboratories

Mavis ANG
Cyber Security Technology Engineer
siewting_ang@sutd.edu.sg

Andrew TAY
Cyber Security Technology Engineer
andrew_taykongngee

TAY Boon Kiat
Cyber Security Technology Engineer
boonkiat2_tay@sutd.edu.sg

General Enquiries
itrust

National Satellite of Excellence

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

Angie NG
Manager
angie_ng

General Enquiries
nsoe_destsci

iTrust
Centre for Research in Cyber Security