Annual Report 2019-2020

National Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructures, Indian Institute of Technology Kanpur

Funded By

Science and Engineering Research Board, Department of Science and Technology, Govt. of India

C3i Center, IIT Kanpur,
208016, Kanpur

Annual Report 2019-20, C3i Center, IIT Kanpur

Contents

Annual Report 2019-20, C3i Center, IIT Kanpur

Executive Summary

The last review meeting was held in September 2019. This progress report summarizes the activities and achievements of the center from September 2019 till August 2020.

The center has several deliverables, namely (i) a national scale SCADA/ICS testbed for cybersecurity studies, (ii) developing tools and techniques for malware collection, benchmarking of malware detection and classification algorithms, (iii) developing tools and techniques for vulnerability, and penetration testing and discovery of yet to be uncovered vulnerabilities in ICS software (iv) developing tools and techniques for insider-threat proofing (v) working with power utilities to build analytic data techniques on PMU data to detect on-going cyber-attacks (vi) creating at least one start-up on the developed technologies (vii) developing mobile malware and their analysis techniques.

In the last one year, the testbed creation in the various critical infrastructure sectors has been accelerated. At this time, all the testbeds have been installed. Power distribution, solar and diesel generation and synchronization, water treatment plant, industrial manufacturing testbeds have all been installed in the lab. The power Transmission

testbed is under installation. The power transmission testbed was supposed to be delivered in April 2020, but due to the COVID-19 related situation, it has been delayed.

The C3i center researchers installed honeypots to collect malware and worked with various researchers around the world to collect sizable repositories of Windows, Linux, Android malware for delivering machine learning-based malware detection, and classification tools. This year the students and engineers at the center published 4 papers in international conferences on malware and botnet detection; 3 more papers are under review. Adversarial training techniques to defeat malware that evade machine learning-based detection by adversarial design have been developed.

In the vulnerability and penetration testing, this year has been quite successful. A total of 14 CVE (Common Vulnerabilities and Exposures) numbers including 7 new, assigned to vulnerabilities, have been discovered and disclosed by the C3i center. Security advisories attributed to the C3i center have been made world-wide by the vendors. Overall, C3i has now made into the league of organizations that contribute to common vulnerabilities and exposures database. Several penetration testing, industrial network traffic capture, and analysis tools have been developed, which are being further developed. A total of 5 papers on testbeds penetration testing and intrusion detection have been published.

Several techniques have been developed and implemented to detect false data injection and data tampering in industrial control networks. On the PLC side, due to resource constraints, invariant failure-based monitoring has been tested and implemented. On the SCADA side, singular spectrum analysis of sensor measurement time series has been implemented. It has also been demonstrated that previous work on singular spectrum analysis has lesser accuracy than our new method. 2 book chapters and 1 international conference paper have been published this year on SCADA security.

A start-up development is under discussion at the moment, and we hope by next year, a start-up would be spawned by the C3i.

We established a long-term strategic partnership with Bharat Electronics Limited (BEL), L&T Technology Services Limited (LTTS), Tech-Mahindra, SMC Corporation (India) Private Limited, Schneider Electric, Synergy to enhance the cybersecurity posture.

A lot of interaction with government agencies such as the National Cyber Security Coordinator, Central Electric Authority, National Thermal Power Corporation, National Highways Authority of India, Tehri Hydro Development Corporation India Limited (Tehri, Uttarakhand), are on-going. Several industries, such as Schneider Electric, Siemens, Tech-Mahindra, LTTS, SMC, have been interacting quite often. Disclosures of vulnerabilities have been made to many ICS vendors – Aveva, Schneider Electric, Rockwell, WAGO and Synergy, in particular.

C3i center also promotes awareness and education in cybersecurity. Yearly cyber-security competition event CSAW, in cooperation with New York University, has been an on-going activity every year. C3i center organized India's first ever Capture-the flag for SCADA (SCADA-CTF) at Nullcon in 2019 and 2020. C3i also hosted 20+ summer interns during the summer who worked for 2 months on various cybersecurity projects. The center also conducted two courses – each of 2 weeks duration, for engineers from various Asian and African countries on the behest of the Ministry of External affairs. A few other training sessions have been organized for various government agencies (not to be named) and students.

C3i, IIT Kanpur, in association with TalentSprint, has designed a six-month Advanced Certification Program in Cyber Security and Cyber Defense for current and aspiring professionals from various organizations who are keen to explore and exploit the latest trends in Cyber Security Technologies. The participants completed the first cohort in Aug 2020. The course allows the participants to combine deep academic rigor and a great practical approach to enable them to master in-demand skills and build world-class expertise.

Message

This is the third issue of the annual report of the C3i Center. C3i center aims at spawning initiatives to develop technology and deploy technological safeguards to protect critical infrastructures. The goal of the center is to create India's first research center whose mission is research, education, and training in the field of critical infrastructure protection and vulnerability studies. Science and Engineering Research Board (SERB), under the department of science and technology (DST) of the government of India, funded the "National Interdisciplinary Center for Cyber Security and Cyber Defence of Critical Infrastructures" (C3i Center) at IIT Kanpur, in March 2017. This annual report covers the period from September 2019 till August 2020.

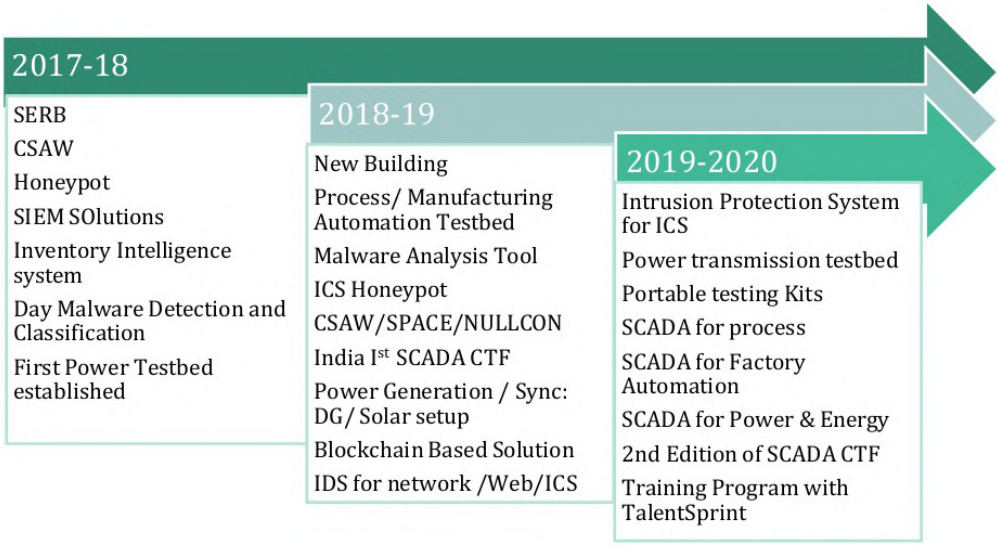
List of Author

Authors	Manindra Agrawal & Sandeep K Shukla
Project Title	National Interdisciplinary Center for Cybersecurity and Cyber Defense of Critical Infrastructures
Security	RESTRICTED (RE)
Version	2.0
Total number of pages	55
Prepared By	Rohit Negi

I

C3i Center

1. History



History of C3i Center

In March 2017, SERB/DST sanctioned the establishment of the National Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructures (also known as 'C3i center'). An amount of 14.43 crores INR was sanctioned over a five year period (March 2017 – Feb 2022) to establish this center as a center of excellence in securing critical infrastructures of the country. In the last few years, it has been recognized for its work internationally.

2. Objective

Major objectives

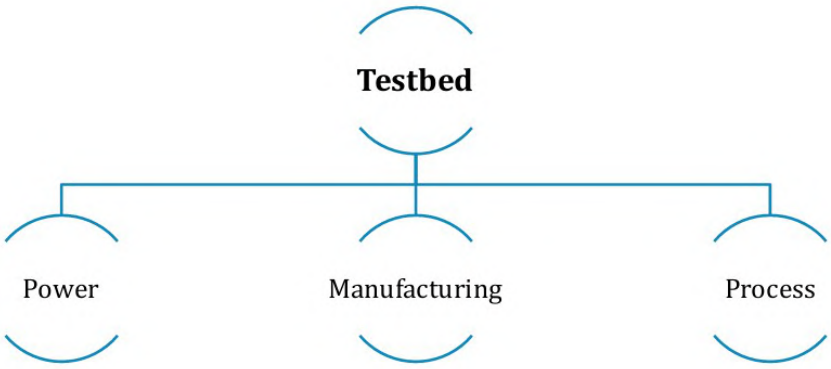
- Design and Development of Machine learning algorithms for detecting on-going cyber-attacks and advanced persistent threats on power systems.
- Build methodology and techniques for deploying honeynets to develop a malware repository and malware analysis and trend forecasting capabilities.
- Apply formal methods to develop effective algorithms for vulnerability and malware detection in applications, systems, and firmware – and transfer such technology to a start-up ecosystem.
- Develop protocol reverse engineering tools and capabilities to detect presence of botnets, trojans and other advanced persistent threats.
- Develop light weight cryptography and block chain-based authentication, identity management and key management schemes for network of devices (IoT and M2M).
- Develop cryptographic co-processors and side-channel proofing techniques for cryptographic hardware, and software systems.
- Field testing security techniques, architectures, and protocols on the IITK smart city project.
- Develop security architecture, perimeter defense, network and Cloud security for critical infrastructure, and inform the policy formulation and best practices guidance for National Critical

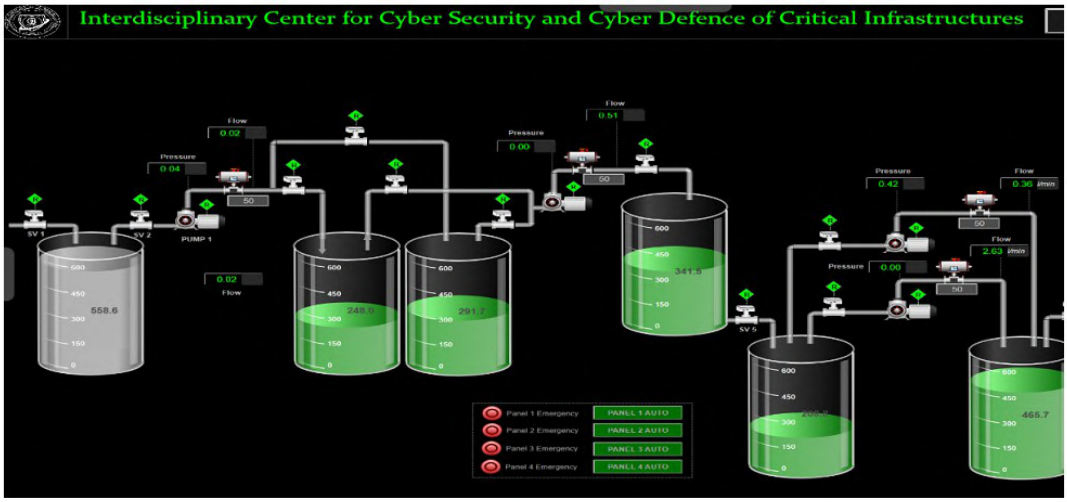
3. Deliverables

- A national scale SCADA testbed for research , training, and hardware/ software in the loop testing by vendor at IIT Kanpur.
- Tools and Techniques for malware collection and benchmark creation for malware analysis.
- Tools and Technique for application software vulnerability detection.
- Tools and technique for insider threat proofing critical infrastructure IT/OT system.
- Work with a power utility or smart grid corporation to experimentally use our PMU data analytics based tools for detecting advanced persistent threats.
- Creation of malware for exploitation of criminal information system and mobiles for offensive security.
- Create at least one start-up with IIT Kanpur incubation enterprise in the cyber of security of critical infrastructure space by licensing IP in vulnerability detection, protocol reverse engineering, malware detecion etc.

4. Infrastructure

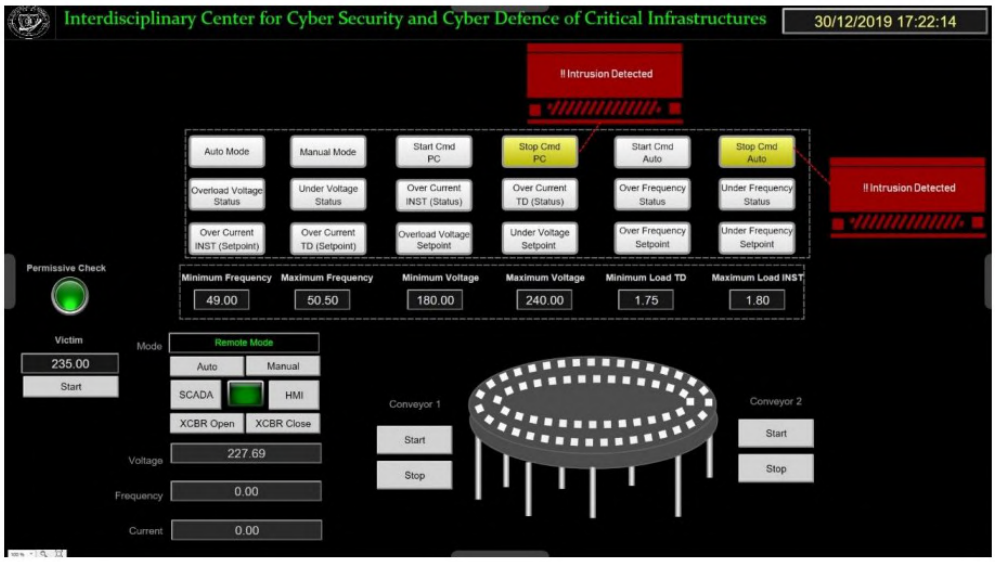
The interdisciplinary center for cybersecurity and cyber defense of critical infrastructures (C3i) at the Indian Institute of Technology Kanpur facilitates researchers to work with the pilot setup of critical infrastructures.





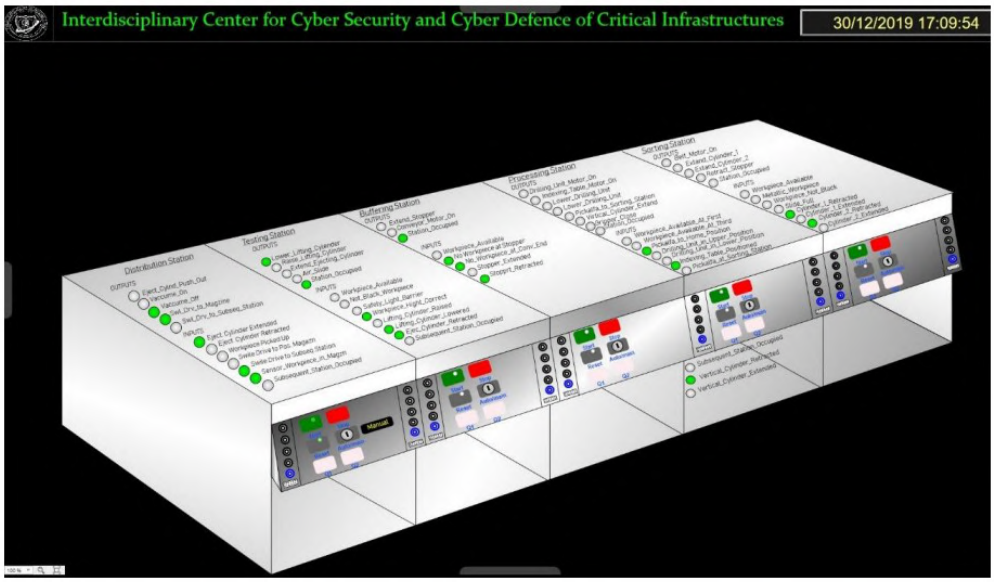
Process Automation

- C3i deployed a centralized visualization, reporting and controlling server for its process automation testbed.
- Front-end mimics the as-built view of the process.
- Visualization of the parameters like flow, pressure, level, etc.
- Alarm and event monitoring and report generation.
- Controlling of actuators like motorized control valve using 4 – 20 mA signal
- Integration of honeypots
- Implementation of intrusion protection system
- This testbed facilitates researchers to design and develop cyber security solutions for process industry.
- Major features of the testbed are data acquisition, remote control, reporting, multiple communication protocols like Modbus, IEC 104, ProfiNet, etc.



Power & Energy Automation

- C3i deployed a centralized visualization, reporting and controlling server for its power & energy automation testbed.
- Front-end mimics the as-built view of the power system.
- Visualization of the parameters like Power, Voltage, Current, Frequency, etc.
- Alarm and event monitoring and report generation.
- Controlling of power dispatch
- Implementation of intrusion protection system



Manufacturing

- C3i deployed a centralized visualization, reporting and controlling server for its manufacturing automation testbed.
- Front-end mimics the as-built view of the manufacturing system.
- Visualization of the states of the manufacturing unit.
- Alarm and event monitoring and report generation.
- Controlling of job
- Implementation of intrusion protection system
- Manufacturing system includes feeding station, buffering station, processing station, sorting station

Portable Kits

- To fulfil an immediate need of "PATCH testing" & hands on "OT security training" kit, C3i center has designed and developed portable kits.
- Kits are rich with industrial protocols, integrated with cybersecurity educational material. It will help critical infrastructures in patch management + inhouse cybersecurity workforce development. Testing kits will allow various technocrats and professionals to get hands-on experience with available cyber technologies for OT and ICS environments.

Power Transmission

- Hard/Software in loop testing facility for power transmission system.
- the key features of 'State of the Art' testing facility is its 100KM long zebra conductor lines as a pi model with 1.1KV 50Hz supply. It will facilitate researchers for testing cyber security innovation.

II

Achievements

5. Vulnerability Assessment

The assessment of hardware and software pertaining to operational technologies in the industrial control system is carried-out at C3i in a controlled environment. Team C3i has successfully identified a large number of vulnerabilities in the products as well as in the systems. A few of them already received international recognition.

Acknowledgement of Responsible Disclosures

- 15+ Responsible disclosures
- Total CVEs published based on C3i disclosures to date : 14
- 7 CVEs published since the last annual report are listed here.

CVE-2019-20046

CVSS v3 9.8 Base Score 9.8 (Critical)

CVSS vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor: SSS (Synergy Systems & Solutions)

Equipment: RTU Vulnerability: The affected product does not require adequate authentication, which may allow an attacker to read sensitive information or execute arbitrary code.

Vendor report: https://www.s3india.com/security_bulletins_rtu.html

ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01

CVE-2019-20045

CVSS v3 9.8 Base Score 7.5 (High)

CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Vendor: SSS (Synergy Systems & Solutions)

Equipment: RTU Vulnerability: Specially crafted malicious packets could cause disconnection of active authentic connections or reboot of device.

Vendor report: https://www.s3india.com/security_bulletins_rtu.html

ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01

CVE-2019-13537/ICSA-19-290-

CVSS v3.0 BASE SCORE 7.5 (HIGH)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Vendor: AVEVA
Equipment: Vijeo Citect software
Vulnerability: The IEC870IP driver for AVEVA's Vijeo Citect and Citect SCADA and Schneider Electric's Power SCADA Operation has a buffer overflow vulnerability that could result in a server-side crash.
Vendor report: https://sw.aveva.com/hubfs/assets2018/pdf/security-bulletin/SecurityBulletin LFSec139.pdf.
ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-19-290-01

CVE-2019-16879

CVSS v3 9.8 Base Score 9.8 (Critical)
CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H
Vendor: SSS (Synergy Systems & Solutions)
Equipment: RTU Vulnerability: The affected product does not require authentication for TELNET access, which may allow an attacker to change configuration or perform other malicious activities.
Vendor report: https://www.s3india.com/security_bulletins_rtu.html
ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01

CVE-2020-7800

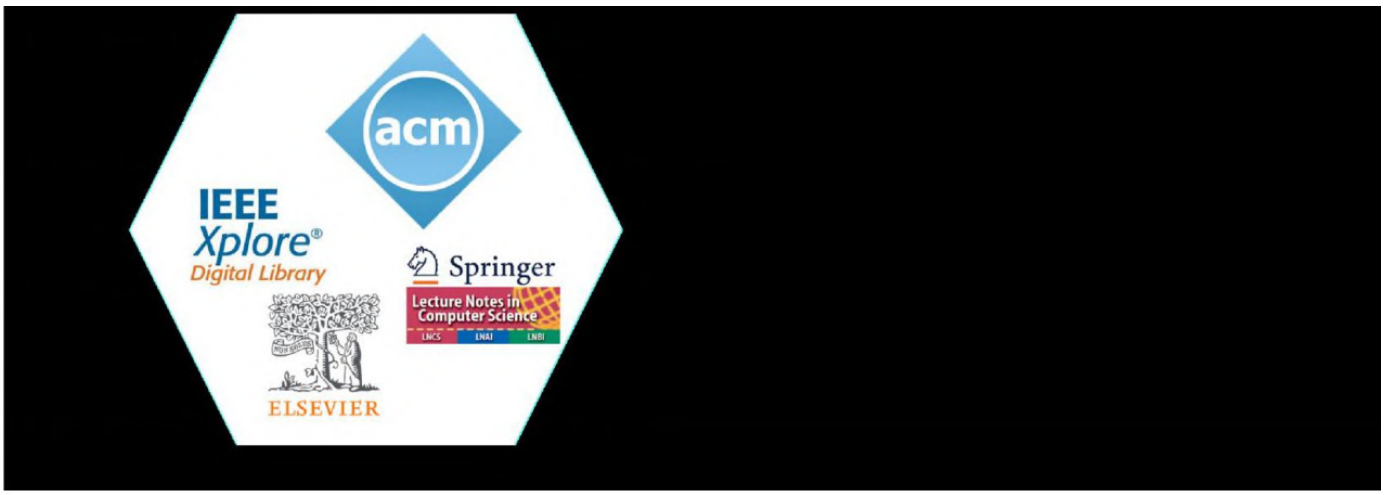
CVSS v3 9.8 Base Score 9.8 (Critical)
CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H
Vendor: SSS (Synergy Systems & Solutions)
Equipment: RTU Vulnerability: The affected product is vulnerable to specially crafted TCP packets, which can cause the device to shut down or reboot and lose configuration settings. Vendor report: https://www.s3india.com/security_bulletins_rtu.html
ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01

CVE-2020-7801

CVSS v3 9.8 Base Score 6.5 (High)
CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Vendor: SSS (Synergy Systems & Solutions)
Equipment: RTU Vulnerability: The affected product is vulnerable to information exposure over the SNMP protocol.
Vendor report: https://www.s3india.com/security_bulletins_rtu.html
ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01

CVE-2020-7802

CVSS v3 9.8 Base Score 9.3 (Critical)CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N
Vendor: SSS (Synergy Systems & Solutions)
Equipment: RTU Vulnerability: The affected product is vulnerable to insufficient default permissions, which could allow an attacker to view network configurations through SNMP communication.
Vendor report: https://www.s3india.com/security_bulletins_rtu.html
ICS-CERT advisory: https://us-cert.cisa.gov/ics/advisories/icsa-20-042-01



6. Publications

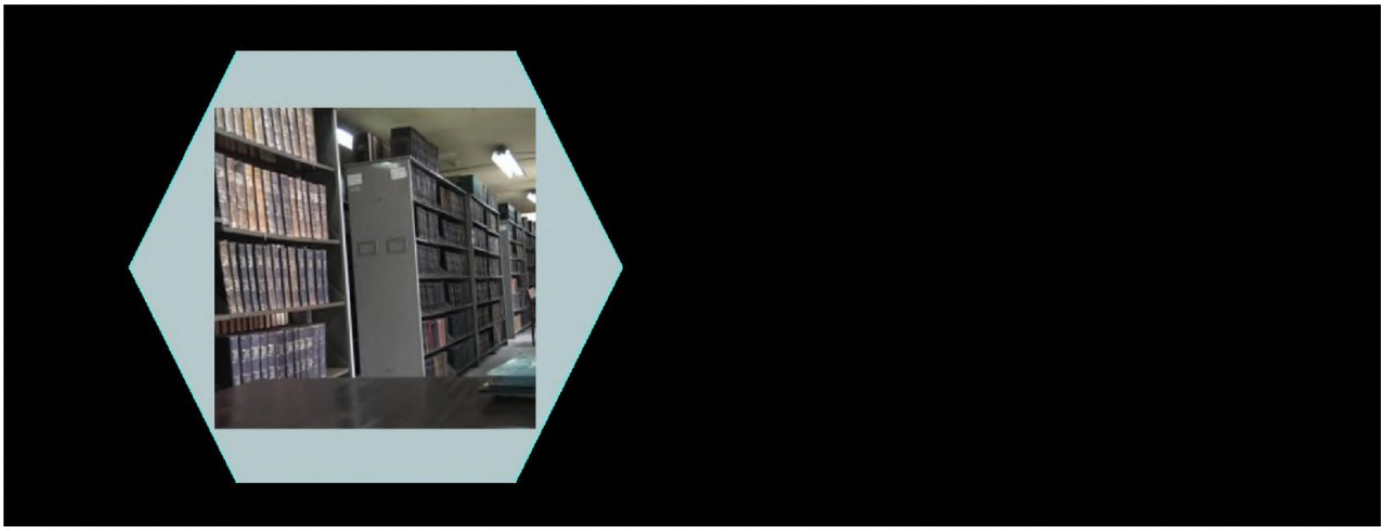
Publications of C3i Center from September 2019 till August 2020.

2020	Rohit Negi, Aneet Dutta, Anand Handa, Ujjwal Ayyangar, Sandeep K Shukla, "Intrusion detection & prevention in Programmable Logic Controllers: A Model-driven Approach," IEEE International Conference on Industrial Cyber-Physical Systems (ICPS 2020), Finland, June 2020.
2020	Venkatesh Subramanian, Yuvaraja Rajendra, Shubham Sahai, Sandeep K. Shukla, "Decentralized Device Authentication Model Using the Trust Score and Blockchain Technology for Dynamic Networks", accepted at 3rd the IEEE International Conference on Blockchain (BLOCKCHAIN 2020), November 2020, Rhodes Island, Greece, 2020 .
2020	Shubham Sahai, Medha Atre, Shubham Sharma, Rahul Gupta, Sandeep K. Shukla, "Verity: Blockchain Based Framework to Detect Insider Attacks in DBMS", accepted at the 3rd IEEE International Conference on Blockchain (BLOCKCHAIN 2020), November 2020, Rhodes Island, Greece, 2020 .
2020	Nitesh Kumar, Ajay Singh, Anand Handa, Sandeep Kumar Shukla, "Detecting Malicious Accounts on the Ethereum Blockchain with Supervised Learning," The 4th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML2020), Be'er Sheva, Israel, 2020.

2020	Rohit Negi, Anand Handa, Sandeep K Shukla. "Building Industrial Scale CyberSecurity Experimentation Testbeds for Critical Infrastructures" in Cyber Security of Industrial Control Systems in the Future Internet Environment, IGI Publisher, Feb2020.
2020	Singh A., Handa A., Kumar N., Shukla S.K. (2020) Malware Analysis Using Image Classification Techniques. In: Shukla S., Agrawal M. (eds) Cyber Security in India. IITK Directions, vol 4. Springer, Singapore.
2020	Kumar A., Gupta M., Kumar G., Handa A., Kumar N., Shukla S.K. (2020) A Review: Malware Analysis Work at IIT Kanpur. In: Shukla S., Agrawal M. (eds)Cyber Security in India. IITK Directions, vol 4. Springer, Singapore.
2020	Rohit Sehgal, Nishit Majithia, Shubham Singh, Sanjay Sharma, Subhasis Mukhopadhyay, Anand Handa, Sandeep Kumar Shukla (2020) Honeypot Deployment Experience at IIT Kanpur. In: Shukla S., Agrawal M. (eds) Cyber Security in India. IITK Directions, vol 4. Springer, Singapore.
2020	Negi R., Shukla S.K. (2020) Building India's First Cyber-Security Testbed for CI. In: Shukla S., Agrawal M. (eds) Cyber Security in India. IITK Directions, vol 4. Springer, Singapore.
2020	Kumar S., Shukla S.K. (2020) The State of Android Security. In: Shukla S., Agrawal M. (eds) Cyber Security in India. IITK Directions, vol 4. springer, Singapore.
2020	Sahai Srivastava S. et al. (2020) Blockchain and Its Application in cybersecurity. In: Shukla S., Agrawal M. (eds) Cyber Security in India. IITK Directions, vol 4. Springer, Singapore.

2020 ·····•	Sandeep K. Shukla. 2020. TECS Editorial: Rethinking and Re-evaluating in the Time of Crisis. ACM Trans. Embed. Comput. Syst. 19, 3, Article 16e (June 2020), 3 pages. DOI: https://doi.org/10.1145/3395923
2020 ·····•	Sandeep K. Shukla. 2020. Editorial: Embedded Computing and Society. ACM Trans. Embed. Comput. Syst. 18, 6, Article 112 (January 2020), 3 pages. DOI:https://doi.org/10.1145/3368250
2020 ·····•	P. V. Sai Charan, Sandeep K. Shukla, and P. Mohan Anand, "Detecting Word Based DGA Domains Using Ensemble Models", accepted at the 19th International Conference on Cryptology And Network Security (CANS 2020), Vienna, Austria, December 2020
2020 ·····•	Saurabh Kumar, Debadatta Mishra, Biswabandan Panda and Sandeep K. Shukla, "STDNeut: Neutralizing Sensor, Telephony System and Device State Information on Emulated Android Environments", accepted at the 19th International Conference on Cryptology And Network Security (CANS 2020), Vienna, Austria, December 2020
2020 ·····•	Rachit Agarwal and Shikhar Barve and Sandeep Kuman Shukla (2020). Detecting Malicious Accounts in Permissionless Blockchains using Temporal Graph Properties, Applied Network Science Journal, Springer.
2019 ·····•	Shukla, S. K. (2019). Adversaries and Robustness. ACM Transactions on Embedded Computing Systems (TECS), 18(4), 30e.
2019 ·····•	Sandeep K. Shukla. 2019. Editorial: Reflections on the History of Cyber-Physical versus Embedded Systems. ACM Trans. Embed. Comput. Syst. 18, 3, Article 19e (June 2019), 2 pages. DOI:https://doi.org/10.1145/3325115

2019 ·····•	Sandeep K. Shukla. 2019. Editorial: Human Factors in Embedded Computing. ACM Trans. Embed. Comput. Syst. 18, 1, Article 1e (February 2019), 2 pages. DOI:https://doi.org/10.1145/3302888
2019 ·····•	Sandeep K. Shukla. 2019. Editorial: Embedded Security Challenge: Cyber Security Contests in the Embedded Computing Domain. ACM Trans. Embed. Comput. Syst. 17, 6, Article 91 (January 2019), 2 pages. DOI:https://doi.org/10.1145/3293502.
2019 ·····•	Rohit Negi and Sandeep K. Shukla, "Cyber Security of Critical Infrastructures: A C3i Perspective", 8th International Conference, SKM 2019 Goa, India, December 21–22, 2019 Proceedings P13-15.
2019 ·····•	Anand Handa, Subhasis Mukhopadhyay, Shankhadip Mallick, Nitesh Kumar, Sandeep K. Shukla, Remish L. Minz, Sanjana Pai Nagarmat, Ramesh Rakesh, "Cyber Risk Assessment of Networked Cyber Assets using Probabilistic Model Checking," 3rd IEEE Conference on Information and Communication Technology, IIIT Allahabad, India, 2019. Awarded as the best paper in the Track: Cyber-Physical Security in Critical Infrastructure.
2019 ·····•	Fenil Fadadu, Anand Handa, Nitesh Kumar, and Sandeep K. Shukla, "Evading API Call Sequence-Based Malware Classifiers," 21st International Conference on Information and Communications Security (ICICS'19), Beijing, China, December 2019.
2019 ·····•	Asan M. Basiri, and Sandeep K. Shukla," LFSR based Versatile Divider Architectures for BCH and RS Error Correction Encoders," Microprocessors and Microsystems, 102902, ISSN 0141-9331, 2019.
2019 ·····•	Hardware Acceleration System, Device and Method for Cryptographic Transactions – IPA 201911049236, Filled on 29/11/2019. Dr. Jubin Mitra (Post-Doc Fellow, CSE), Dr. Sandeep K. Shukla (CSE), Dr. Manindra Agrawal (CSE).



7. Thesis

Thesis submitted from October'19 to August'20

1 ·····•	Design, Implementation, and Protection of Critical Cyber-Physical System Testbeds for Cyber Security Research. Rohit Negi (16111404) MS Research (2020).
2 ·····•	Detecting Malicious Accounts in Permissionless Blockchains using Temporal Graph Properties. Shikhar Barve (18111065) MTech (2020).
3 ·····•	Investment Compliance in Hedge Funds using Zero-Knowledge Proofs on Ethereum. Komal Kalra (18111032) MTech (2020).
4 ·····•	HoneyBadgerBFT as an ordering service in Hyperledger Fabric. Deepak Yadav (18111015) MTech (2020).
5 ·····•	Symbolic Execution Tool to find DoS Vulnerabilities in Ethereum Smart contracts. Deepak Yadav (18111014) MTech (2020).
6 ·····•	Adversarial Attacks Against Dynamic API Calls Based Malware Classifiers. HariOm (18111019) MTech (2020).
7 ·····•	Prometheus: A Protocol Testing Framework for ICS Protocols. Siddharth Kumar (18111068) MTech (2020).

III

Outreach

8. Collaboration

The following below collaborations were initiated this year (2019-20).

L & T Technology Services Limited

Bharat Electronics Limited

SMC Corporation (India) Pvt. Ltd.

Synergy System & Solutions

Tehri Hydro Development Corporation (THDC)

National Highway Authority of India (NHAI)

भारतीय राष्ट्रीय राजमार्ग प्राधिकरण
National Highways Authority of India

HCL Technologies Limited

9. Events

Team C3i actively organizes cybersecurity events, as mentioned. C3i also participating in organizing events, tutorials and exhibits various cyber security events

CSAW in collaboration with

NEW YORK UNIVERSITY

Grenoble INP

UNIVERSIDAD IBEROAMERICANA CIUDAD DE MÉXICO

INDISEC 2020: CYBER & INTERNAL SECURITY" Summit

NULLCON CONFERENCE 2020

Data Security Council of India (DSCI) Summit 2019

10. Training

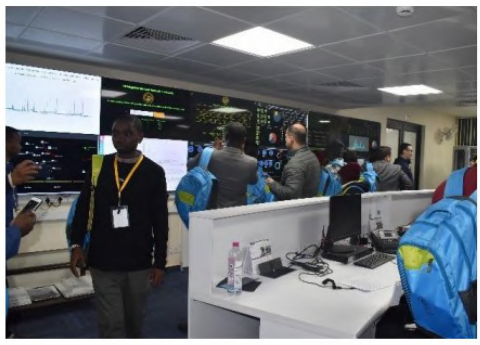
Team C3i provided training to the international IT workforce under the ITEC program of the ministry of external affairs.

Hands-on training to students from different-different countries

- BHUTAN
- BANGLADESH
- CAMERON
- FIJI
- GHANA
- EGYPT
- ETHIOPIA
- IRAQI-KURDISTAN
- KAZAKHSTAN
- LAOS
- MAURITIUS
- MONGOLIA
- MOROCCO
- MOZAMBIQUE
- NIGERIA
- OMAN
- PALESTINE
- SOUTH SUDAN
- SRILANKA
- SUDAN
- SIERRA
- LIONS
- SEYCHELLES
- SYRIA
- TANZANIA
- UGANDA
- UZBEKISTAN
- VIETNAM
- ZIMBABWE

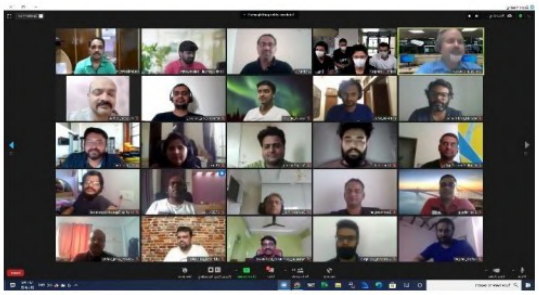

Indian Technical & Economic Cooperation Programme
Training Course
" Introduction to Cyber Security "

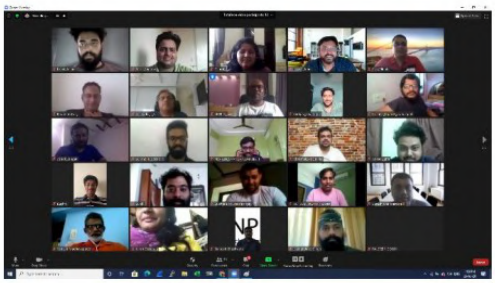

NEVER GIVE UP

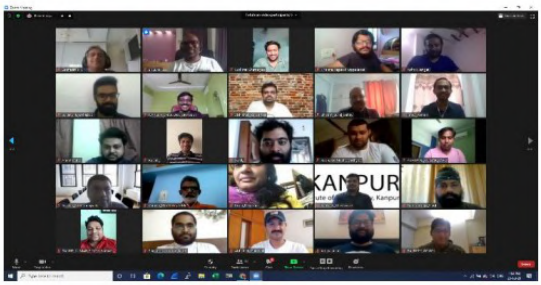


Cyber Security course for Executives in collaboration with

talent sprint







11. Lab Visits at C3i Center

Shri Ramesh Pokhriyal Nishank, Minister of Human Resource Development (MHRD), visited C3i center IIT Kanpur.

ADG of Uttar Pradesh (U.P) Police visited C3i center IIT Kanpur.

Prof. Lamine Mili, from Virginia Tech, -- an IEEE fellow and a renowned expert in Power System State Estimation, visited the C3i center.

Prof. Arvind, from Massachusetts Institute of Technology (MIT), visited C3i center IIT Kanpur

Defence Corridor (Govt. of India) visited C3i center IIT Kanpur.

Intel Corporation visited C3i center IIT Kanpur.


Houston University visited C3i center IIT Kanpur.


National Thermal Power Corporation Limited (NTPC) visited C3i center IIT Kanpur.


Schneider Electric visited C3i center IIT Kanpur.

Chief of Cyber Security of INDIA, visited C3i center IIT Kanpur.

Texas University visited C3i center IIT Kanpur.

Science and Engineering Research Board (SERB) visited C3i center IIT Kanpur.




L&T Technology Services Limited (LTTS) visited C3i center IIT Kanpur.





Indian Institute of Technology Kanpur
C3i
Center