Detailed Project Report

for

C3iHub

by

IIT Kanpur

1 Contents

2 Executive Summary

The Hub

The proposed Hub aims to address the issue of cyber security of cyber physical systems *in its entirety*. From analysing security vulnerabilities and developing tools to address them at various levels of system architecture, to translating these tools to deployment-ready software, to nucleating start-ups developing these tools at scale, to partnering with industries in this domain and co-development and transfer of these technologies, to training the next generation of cyber security researchers and professionals.

Intellectual Focus

A cyber physical system can be divided into nine layers, each of which is vulnerable to different forms of cyber-attacks. These nine layers are:

Hardware layer: processors, storage devices etc. Vulnerable to side channel attacks and hardware trojans

Micro-architecture layer: execution of machine language instructions. Vulnerabilities come due to attempts to speed up execution

Firmware layer: instruction set for booting and security patches. Vulnerable to use of malicious firmware due to false certification

Operating System layer: program that controls functioning of whole computing system. Vulnerable to security holes in the code

Network layer: protocols that enable communication between computers. Vulnerable to security holes in the code

Application layer: software implementing specific application. Vulnerable to security holes in the code, and weaknesses in design of software

Distribution layer: software to manage application distributed over multiple computers. Vulnerable to security holes in the code, and weaknesses in design of software

System Architecture layer: design of the entire automation setup for a cyber physical system. Vulnerabilities arise due to even one component being weak.

Physical Dynamics layer: dynamics of entire system. A clever cyber-attack may not be detectable by observing just one component, rather it requires analysing the dynamics at multiple points of the system.

The work in the Hub will encompass all the above nine layers: analysing various vulnerabilities and developing tools for addressing them. Three types of cyber physical systems will be in focus to being with: Critical Infrastructure (power generation and distribution, water distribution, Industry 4.0 etc.), Automotive Systems (cars etc), and UAVs (drones of various sizes and ranges).

Proposed Activities

1. Analysis of security vulnerabilities in all the above layers with respect to the three types of cyber physical systems mentioned above.
2. Development of tools to address these vulnerabilities.
3. Translation of these tools to deployment-ready software, and nucleating start-ups deploying these tools
4. Partnering with industries in security domain and co-development and transfer of cyber-security technologies
5. Creating extensive courseware on cyber security to be used for training next generation, and generating simple but effective prescriptions for common population to follow

Integration

The Hub will be in IIT Kanpur which already has well-developed components to enable above activities. These include a Center for Cyber Security of Critical Infrastructure (C3i), an Incubation Center (as a Section 8 company), a Technopark enabling industry collaborations (as another Section 8 company), and a media center that has expertise in developing MooCs and other online courseware. Three collaborating partners from India will help substantially at the various layers where they have the right expertise. Foreign collaborators will also have substantial impact on the research agenda. The Industry partners will provide the pathway to understanding the industrial needs, as well as in some cases productization of the developed tools and provide services based on the methodologies and standards developed.

Short and Long-term Research and Translation Goals

In the short term, the work being done in C3i center on security vulnerabilities of critical infrastructure will be expanded to include automotive and UAV sectors. Also, a masters program in cyber security will be launched at IIT Kanpur.

In the long term, (i) hardware testing lab will be created to test presence of trojans and side channels in imported hardware, (ii) work on all nine layers and three sectors will be initiated, (iii) security analysis of model cryptographic algorithms like RSA, ECC, Lattice-based etc will be done with an aim to find weaknesses in them, (iv) at least twenty-five start-ups will be nucleated taking various technologies developed at the Hub to the market, (v) co-development of technologies will be done with at least ten companies in the three sectors, (vi) ten courses on various aspects of cyber security will be developed on online platform and offered as MooCs, (vii) wide range of awareness and executive training programs will be launched along with faculty and student training programs.

3 Context/Background

This document provides a detailed description of activities at the Technology Innovation Hub (TIH) being set up at IIT Kanpur on cybersecurity and cybersecurity of physical infrastructure. The name of the hub will be **C3iHub** where standing for "Cybersecurity and Cybersecurity of Cyberphysical systems Innovation Hub".

3.1 Cyber Security in India

"A Cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets"

- Notification on National Cyber Security Policy-2013 (NCSP-2013)

The 2013 National Cyber Security policy notification captures the essence of the urgent need for indigenous research on cyber security and cyber defense, as Richard Clarke had articulated that the next frontier for national defense is the cyber frontier. While countries such as the US, UK, European nations, Russian Federation, China, Japan, South Korea etc., are all working on developing technologies to protect their cyber-space, often the tools and techniques developed for their purposes are export restricted. As a result, even when certain cyber defense technologies are commercially available, the ones that are most required are often beyond the reach of other nations. For example, a number of commercial static software analysis tools developed by companies such as GrammaTech, Klocwork, or Coverity are export restricted in the United States.

Further, as Section G of *NCSP-2013* rightly emphasizes on, protection of critical infrastructure from cyber-attacks is the greatest concern of most nations today. This concern led to the 2013 presidential executive order by the US President specifically related to the cyber-security of critical infrastructures such as power grid, manufacturing automation, transport system, air-traffic control, nuclear generation facilities, chemical plants etc., all of which are vulnerable to possible cyber-attacks, even in the presence of sufficient air-gap as shown in the case of Stuxnet worm attack on the Iranian nuclear enrichment facilities. In 2014, a German Steel plant's control infrastructure was damaged through a cyber-attack [as reported by the Germany's Federal Office for Information Security. In a recent incident in October 2019, a nuclear power plant in India was found to be victim of a cyber-attack with a malware in its IT system which fortunately did not make its way to the control system network of the plant. These kinds of attacks on critical control systems are likely to increase in number and sophistication as the Business network and the control network are being merged due to the IP-convergence by virtue of which the business functions and manufacturing or other critical functions are being controlled, and monitored via a convergence of traditionally two air-gapped networks. More ominous was a 2015 discovery by the researchers at the Kaspersky lab that a group of operators code named "Equation Group" possibly connected to the US National Security Agency (NSA) has infected computers and information networks in at least 42 countries, which includes India, with malware which were inserted into CDs and USBs in transit via postal mail for

standard commercial software, intercepted during mail transit, manipulated, and then again resealed and forwarded to original destination.

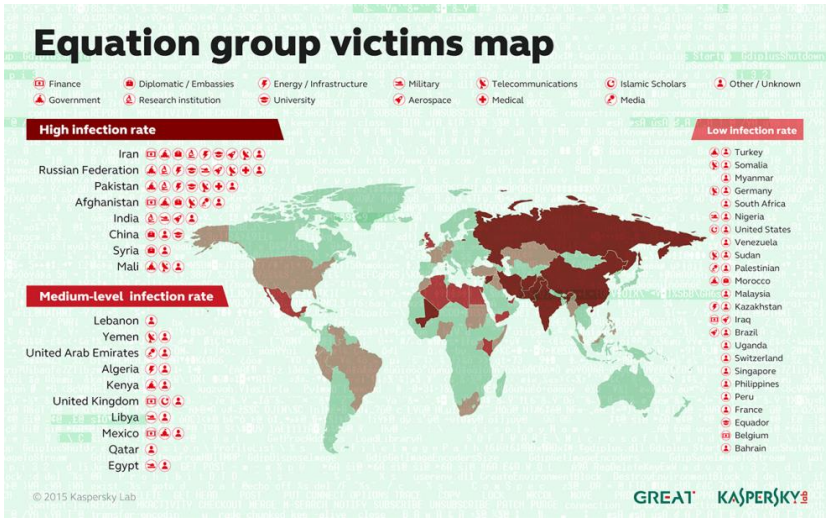
An additional cause for concern is that India imports nearly all of its hardware, and there is always a risk that some of these may have backdoors allowing a foreign country to eavesdrop into the information on a computer or a network.

Error! Reference source not found. shows that in India the Equation group infected telecommunication, research institutes, military, and other information infrastructures over one and half decades preceding its discovery, and among the 8 countries with the highest infection rate, India ranks fifth.

As a result, there is an urgent need for:

i) Research in cyber threat modeling, security policy and technologies, and cyber-defense mechanisms to protect the critical infrastructure on which the national security and national economy depends heavily,
ii) Development of expertise in critical infrastructure cyber defense to help the government in creating policy and small business entrepreneurship incentives to develop indigenous cyber security industry,
iii) Development of tools that can test the presence on backdoors in hardware as well as sandboxes that secure a system in an insecure environment,
iv) Creation of standards and best practices documents for the government and industry,
v) Development of man-power educated, and trained to serve in operational roles for cyber security and defense, as well as for future research,
vi) Creation of awareness and training of private and public sector businesses involved in creating, managing, and maintaining critical infrastructure such as electric power companies, state electricity boards, the various regulatory agencies, the industries with high level of industrial automation, railways, air traffic control, nuclear power and other power station owning businesses etc., and
vii) Recruitment of faculty with expertise in cybersecurity in universities across the country, and train college and university faculty at engineering colleges throughout India on cyber security education, research, and man-power development.

Figure 1: Equations Group Victims Map



3.2 The Proposed Hub

The proposed Hub aims to address the issue of cyber security of cyber physical systems *in its entirety*. From analyzing security vulnerabilities and developing tools to address them at various levels of system architecture, to translating these tools to deployment-ready software, to nucleating start-ups developing these tools at scale, to partnering with industries in this domain and co-development and transfer of these technologies, to training the next generation of cyber security researchers and professionals.

4 Activity Plan

This section provides details of the activities planned and methodologies to be adopted for the same.

4.1 Overview

6. Analysis of security vulnerabilities in all the abstraction layers (see below for details).
7. Development of tools to address these vulnerabilities.
8. Translation of these tools to deployment-ready software, and nucleating start-ups deploying these tools.
9. Partnering with industries in security domain and co-development and transfer of cyber-security technologies.
10. Creating extensive courseware on cyber security to be used for training next generation, and generating simple but effective prescriptions for common people to follow.

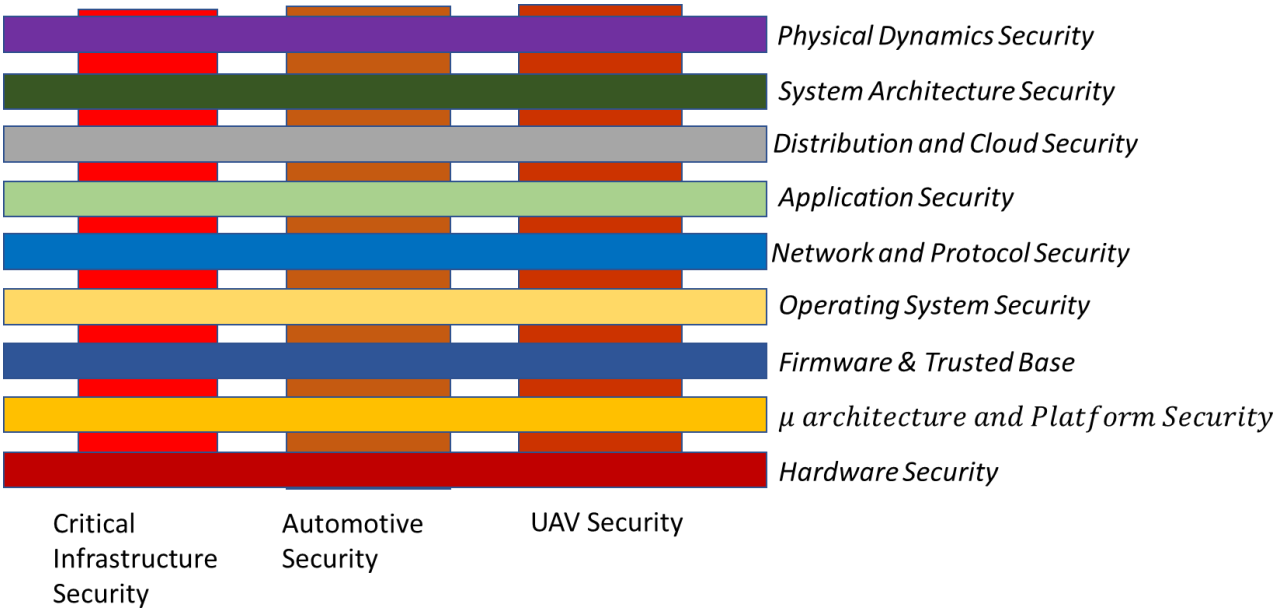
4.2 Integration

The Hub will be in IIT Kanpur which already has well-developed components to enable above activities. These include a Center for Cyber Security of Critical Infrastructure (C3i), an Incubation Center (as a Section 8 company), a Technopark enabling industry collaborations (as another Section 8 company), and a media center that has expertise in developing MooCs and other online courseware. Apart from work at IIT Kanpur, the Hub will support security research and development at institutions across the country, with three collaborating partners already on board to help substantially at the various layers where they have the right expertise. Foreign collaborators will also have substantial impact on the research agenda. The Industry partners will provide the pathway to understanding the industrial needs, as well as in some cases productization of the developed tools and provide services based on the methodologies and standards developed.

4.3 Planned Activities

4.3.1 Knowledge Generation

Figure 2: Domain Verticals and Horizontal Technology Layers



4.3.1.1 Introduction

The Cyber Security Technology Innovation Hub plans to carry out research in cyber security and cyber defense of three domain verticals – namely critical infrastructure cyber physical Systems (CI-CPS), Automotive Control (A-CPS), and Unmanned Aerial Vehicles Control (U-CPS). All these verticals are cyber physical systems in their own ways – but have different scales and scopes of cyber-attacks on them.

Critical Infrastructure CPS (CI-CPS): A critical infrastructure CPS such as power generation, transmission or distribution systems span large geographical areas, have physical dynamics that are affected by components which are far apart in geography, and the control is hierarchical based on utility area control, state level load dispatch control, sub-grid level control (e.g., load dispatch centers for the five sub-grids – northern, eastern, western, north-eastern and southern grids in India), and overall control via the central load dispatch center. Other critical infrastructures such as water treatment plants, sewage treatment and control in municipal areas, or a factory automation in a factory scale scope, are also distributed, multi-stage, heterogeneous control-based CPS – but have a different impact levels in case of cyber-attacks.

Automotive CPS (A-CPS): In automotive CPS, the control is mostly confined within an automotive, even though modern automotive have close to 100 processors, multiple network clusters with bridges between them, and often in modern day cars – interaction with GPS, or other types of satellite-based communication mechanism. However, it has been shown in the recent research that control systems in cars have often exposed cyber-attack surfaces through which a car can be hijacked, it's control can be

compromised, response time may be rendered too slow for breaks to engage. Even GPS spoofing and other techniques could lead a car to wrong directions.

Unmanned Aerial Vehicle CPS (U-CPS): In the unmanned aerial vehicle domain, there are multiple different components – on board flight control platform, remote operation and monitoring, the flight module service, the flight module client, flight management server, and finally the regulatory servers – all would be targets for cyber-attacks.

4.3.1.2 Cyber Security of Horizontal Technology Layers

In order to develop cyber security technology specific to these domains, there are certain common horizontal technology layers we have identified, which need to be developed independent of these vertical domains and then the technology and knowledge thus developed can be customized for each specific domain.

The layers we focus on are shown in **Error! Reference source not found.** . They are as follows:

Hardware layer – the attack surface exposes through side channels such as power usage variation, electromagnetic variation, timing variations – which allows attackers to decipher secret cryptographic keys – which can then expose all the upper stack which may depend on cryptographic means of confidentiality and authenticity. The other issue that needs to be tackled at the hardware layer is implanted Trojans while fabricating the hardware chips – as that could create a persistent threat at the very basis of any security built into the system through upper layers. Hardware implementation of cryptographic algorithms and protocols are also part of this layer. In the proposed TIH – this layer will be led by Prof. Sandeep Shukla of C3i lab with the help of our collaborators from IIT Kharagpur. In Summary, major issues to tackle at this layer are

i. Side Channel Analysis and Proving non-existence of significant side channels in hardware deployed in CPS
ii. Testing for Trojan logic in the chips
iii. Side Channel free hardware implementation of Cryptographic Algorithms for fast and secure cryptography
iv. Leader of the work in this layer will be Prof. Debdeep Mukhopadhyay from the SEAL lab in IIT Kharagpur.

Micro-architecture and Platform Architecture – the attack surface at this layer are many – mostly through micro-architectural and platform vulnerabilities. Examples of such problems surfaced most recently with Intel processors with Meltdown and Spectre vulnerabilities. These were exposed because of aggressive micro-architectural optimizations such as use of out-of-order execution of instructions in processors. Platform architecture includes the memory architecture, the interconnection network in multiprocessor chip, and various protocol interfaces. These also use aggressive micro-architectural optimizations and in the recent past researchers have been finding various security flaws most of which either breach confidentiality of data in memory, or in cache hierarchy, or can even create disruption or data integrity challenges.

In this layer, the work will be mostly led by IIT Kanpur's micro-architecture and memory system experts with IIT Kharagpur collaboration. In summary, the major problems to consider at this layer are:

i. Micro-architectural optimizations which lead to cyber vulnerabilities
ii. Platform architecture designs and optimizations exposing security vulnerabilities

The leader in this layer will be Prof. Biswabandan Panda from IIT Kanpur's Computer Architecture Research for Resilient, Secure and Scalable Systems (CARS Lab). Foreign collaborator in this layer will be Prof. Ramesh Karri and Prof. Ozgur Sinanoglu – from New York University.

Firmware and Trusted base -- The firmware of any processor, programmable logic controller (PLC), Remote Terminal Unit (RTU), routers and other Industrial IoT devices are pieces of low-level software that is responsible for booting the device to implementing various functions that employ simpler instructions to implement functions in lieu of more complex instructions. The firmware is also the mechanism through which security patches are made to devices when a hardware level vulnerability is discovered. As a result, security of firmware is very important from various threat possibilities – for example, secure boot of the device, authenticity of firmware patches, vulnerabilities of software – such as buffer overflow, and the certification of the authenticity of firmware. It turns out that in many well-known attacks, firmware update with falsified digital certificates purportedly from the original developer of the firmware played a significant role in the attack (e.g. STUXNET). Also, to boot-strap trust in a system that is otherwise untrusted, a trusted computing base (TCB) is implemented in modern devices. The trusted base is implemented in hardware and firmware combination, and all trusted computing in other layers derive the trust by the security of the TCB implementation. In recent times, our colleague from IIT Kanpur, Prof. Pramod Subramanyan has shown that certain security assumptions in enclave architectures which are used as trusted base of software processes in modern Intel processors may not all hold.

Another threat of work in this layer is cryptography, multi-party computation, and cryptographic protocols for security and trust. This thread will be led by Prof. Manindra Agrawal from C3i Center of IIT Kanpur, and Prof. Arpita Patra of IISc Bangalore.

This work in this layer will be led by Prof. Pramod Subramanyan along with collaborator from IISc, Bangalore Prof. Vinod Ganapathy. Prof. Ozgur Sinanoglu from New York University will partner in this activity as well.

In summary, some of the major issues at this layer are:

i. Secure Boot methods and Proving Security Properties of Secure boot
ii. Firmware and firmware patch trustworthiness and authenticity
iii. Vulnerability discovery of firmware
iv. Vulnerability of Enclave architectures and other TCB architecture
v. Cryptography, Multi-Party Computation, and Light-weight Cryptography

Operating System Security – Operating systems are often exposing severe vulnerabilities. The dirtyCOW vulnerability in Linux Kernel in 2016 – exposed all derived operating systems such as Android, RT-Linux

etc., to the same vulnerability which could be exploited for privilege escalation leading to compromise of all security of the device and other devices in the network. Earlier in 2019, VxWorks – one of the most widely used real-time operating system in CPS sector was found to have a severe vulnerability by Armis Labs. There were 11 vulnerabilities disclosed which left billions of devices in various critical infrastructures, automotive systems, and avionics systems exposed until they were patched. As a result, one of the major thrusts of research has to be in operating system security – finding vulnerabilities, customizing existing operating systems by restricting APIs for system calls in order to reduce the attack surface, and also to apply formal methods to prove security properties of various system call APIs. Vulnerability of Kernal design (such as DirtyCOW) could have been exposed through formal modeling.

The work in this layer will be led by Prof. Debadatta Mishra and Prof. Pramod Subramanyan in IIT Kanpur will collaboration from Prof. Vinod Ganapathy at IISc Bangalore. The foreign collaborator at this layer will be Ben Gurion University in Israel. In summary, some of the issues to be tackled at this layer are:

i. Formal Model Driven Fuzz Testing to discover operating system vulnerabilities
ii. Vulnerability and Penetration Testing Methodology and tools
iii. Security of System Call APIs
iv. Security of Device Drivers
v. Customizing existing O/S with minimal attack surface
vi. Formal proofs of security properties
vii. Trusted Operating System by boot strapping trust from TCB and formal proofs of trust properties
viii. Host Based Intrusion Detection

Network and Protocol Security – At the network interface through which communications happen – depending on the device – there are often implementation of industrial protocols such as ModBus, IEC 61850, IEC 60870-5 104 protocol, OPC protocol – or general TCP/IP. Also, for processing elements in automotive CAN (Control Area Network), or Flexray, or in the UAV domain – UAV CAN. Some of these protocols have inherent vulnerabilities – especially industrial control protocols – as they are neither encrypted nor authenticated. These protocol shortcomings themselves expose us to MITM (Man-in-the-Middle) attacks, unauthenticated command execution, unauthenticated password recovery etc. Even those protocols which provide for encrypted payloads, and digital signatures, often either the protocol interaction has flaws in terms of security – for example – famous Needham Schroder protocol flaw. Also, timing signals for synchronization often plays important role in CPS system coordination, and alignment of sensor data per time point. GPS, Rigbee and other timing signal protocols often have vulnerabilities such as GPS spoofing, jamming, and other attacks. As a result, to secure CPS – one has to work towards better protocol definition, secure implementation, detection of on-going attempts to compromise, and response mechanisms – all are important component of secure and Resilient CPS design.

At IIT Kanpur – this work will be led by Prof. Ketan Rajawat from Electrical Engineering department along with researchers from C3i Center at IIT Kanpur. The foreign collaborators will be from New York University, Tel Aviv University and Ben Gurion University of Israel. Major issues to tackle at this layer are:

i. Protocol Vulnerability Studies

ii. Light-weight cryptography for Real-Time Protocols
iii. Security of Industrial Protocol Implementations
iv. Vulnerability and Penetration Testing for Finding Protocol Implementation Vulnerabilities
v. Secure Network Architecture for CPS
vi. Surveillance of Network Traffic
vii. Timing and Location Signal Security – Spoofing, Jamming
viii. TCP/IP Security, DNS Security, BGP Security etc.
ix. Perimeter defence mechanism
x. Network based Intrusion Detection

Application Security – this is one of the most challenging part of security – as off-the-shelf and vendor-built applications are often installed on CPS control, monitoring, archiving of historic data for further data analytics, state estimation, N-1 Contingency analysis etc. In Automotive, applications range from entertainment system to drive-by-wire control mechanism in software. In UAV similarly, there are multiple applications both on-board and ground stations. Applications tend to have software implementation vulnerabilities such as buffer overflow, string format vulnerability, integer overflow, heap spraying vulnerability etc. These are often exploited to escalate privilege and thereby make inroads into the network interface whereby a worm style malware can compromise the other critical functionalities such as control, breaking mechanism etc. Steve Savage's group in UC San Diego showed how a buffer overflow vulnerability in a car's entertainment system enabled them to take over the anti-lock braking mechanism of a car. The application vulnerability may be not only due to software bugs, but also in algorithmic design (state estimators in power system have been shown to have vulnerabilities if the attacker has knowledge of the system topology and parameters), in the software architecture and its dependence on privileged access to system kernel, in the control algorithms leading to destabilizing control, or in relaying mechanism such as the role of Zone-3 relays in power system in aggravating a cascading blackout. Extensive research is required for vulnerability analysis, development of tools and methodologies for automated vulnerability discovery and penetration testing, development of secure patching mechanism to prevent attacks by unauthorized and unauthenticated patches. The need for analysis of malware and classification of malware automatically using machine learning is also part of this layer. Creating Application specific firewall which regulates application specific protocol traffic and API calls using machine learning based approaches is another thread of research in this layer. Application specific honeypot creation for entrapment of attackers to collect threat intelligence, modus operandi of the attackers, collecting malware – is another area to develop in this layer. Another area we plan to pursue is formal modelling and formal verification (both model checking and program analysis techniques) to find security bugs in the applications.

Activities in this layer will be led by Prof. Sandeep Shukla from C3i Center, IIT Kanpur with collaboration from Prof. Soumyajit Dey of IIT Kharagpur, and foreign collaborator from Tel Aviv University.

The major thrusts of research this layer is:

i. Application vulnerability assessment and penetration testing

ii. Formal Methods and Verification Techniques for finding vulnerabilities, and proving security guarantees in application
iii. Application Specific firewalls for regulating application specific protocol interactions as well as API calls (this includes web application firewalls)
iv. Honeypots for collecting application specific threat intelligence
v. Secure patch management of applications etc.

Distribution and Cloud Security – most CPS systems are not monolithic control applications – but rather distributed computing systems with hundreds to thousands of devices (such as PLCs, RTUs, IIOTs, SCADA workstation etc., in case of critical infrastructure, processing elements over multiple communication buses in automotive and avionics). As a result, an attack on a single device in the distributed system can cascade to others. For example, in case of a worm – it can traverse the network from device to device and create a macro-level attack. Example of that was STUXNET, but also recent ransomware attacks – for example, NotPetya worked in similar fashion. The NotPetya entered the Maresk shipping system's network by virtue of an automated patch for a popular desktop accounting application in Ukraine. Since there Maresk network spans over 130 countries, from that single attack point, it encrypted and bricked thousands of machines belonging to their network all over the world, including the Microsoft active server files – which disabled their entire authentication system worldwide. Another growing trend for CI-CPS utilities is to collect industrial control network data into cloud in order to obtain analytics for further optimization of processes, and for business information, inventory management etc. This opens a very ripe attack surface from the cloud environment to the infrastructure – because if the cloud is not on a secure server with patched operating system, hypervisor, and network interfaces, one could be infiltrated from the cloud environment and then run havoc on the entire network including the field network. The attack on Target supermarket chain happened through a cloud-based service for their HVAC system which provided remote access to HVAC vendor – while the attack in that HVAC monitoring and analytics system eventually infiltrated the point-of-sales devices network – and stealing customer information of 13 million customers. Therefore, authentication, and authorization architecture, secure remote access into devices of the CPS system, securing the Industry automation architecture of the distributed multi-layer networked system, securing the cloud to infrastructure network interface (e.g. implementing data diodes) – are some of the major areas of research in this layer.

Prof. Debadatta Mishra, Prof. Pramod Subramanyan, Prof. Sandeep Shukla will lead research in this layer along with Prof. Vinod Ganapathy at IISc, Bangalore. Foreign collaborator in this activity will be from the ICRC (Blavatnik Interdisciplinary Cyber Security Research Center) at Tel Aviv University, and also from the University of California at San Diego.

The major research topics at this layer are:

1. Securing the authentication and authorization architecture in the distributed system
2. Threat modeling and threat analysis framework for large scale distributed CPS
3. Secure virtualization in Public as well as Private Cloud
4. Multi-party computation-based sharing of secret keys

5. Cloud Security – especially securing the interface between cloud collecting data and the critical devices and network – i.e. developing data-diodes
6. Secure virtualization etc.
7. Use of block-chain for tamper proof logging system wide events with time stamping
8. System Level intrusion detection by correlating events from various components of the system

Securing System Architecture – this is the all-encompassing layer that defines overall security architecture of an entire factory automation, or a geographically distributed power grid, or a nuclear generation facility etc. If the system architecture has weaknesses, then securing all the other layers may not be very useful. For example, 30% of all major attacks are known to be insider attacks. Securing the perimeter, securing the individual devices may not be enough against an insider attack especially a privileged insider. Therefore, the system architecture must be built to be resilient against attacks. Resiliency means (i) the system should be able to detect an ongoing attack as soon as possible (worldwide average detection for unprepared utilities is close to 260 days which means that by that time the attack has persisted into the system and possibly waiting for an opportune moment to strike); (ii) system must be able to contain the attack by islanding the affected part of the system; (iii) respond to the attack by islanding as well as enhancing and regulating activities in so far unaffected part of the system; and (iv) recover as quickly as possible. The resiliency is not about protection but more about monitoring and surveillance for fast detection, response and recovery.

We plan to build methodologies, system architecture frameworks and tools that would allow us to build resilient CPS – also, we must have a pathway to build resiliency in already existing CPS installations by retrofitting solutions we plan to develop.

In this, we follow security architecture standards such as ISA/IEC 62443 and NIST (National Institute of Standards and Technology, USA) Cyber Security Framework (CSF).

The lead for this layer will be Prof. Sandeep K. Shukla of C3i Center. The domain experts in Automotive Prof. Soumyajit Dey in IIT KGP, and Prof. A. K. Ghosh in the Aerospace engineering department of IITK will provide the domain specific inputs to secure system architecture for Automotive (e.g. AUTOSAR), and UAVs. IoT architecture work will be carried out by Prof. S. Venkatesan of IIIT Allahabad with IIT Kanpur and IIT Kharagpur colleagues.

The main research activities in this layer are:

i. Methodology development for Secure System Architecture based on Standards for CI-CPS, A-CPS, and U-CPS
ii. Tools to support NIST cyber security framework implementation (Detection, Isolation and Islanding mechanism, Response mechanism and Recovery Mechanism)
iii. Advisories for Industry and Utilities
iv. Securing large-scale IoT and IIoT ecosystems.

Physical Dynamics Layer – For cyber physical systems – often the cyber-attacks are not isolated or a single vulnerability exploitation but many vulnerabilities in different devices, network, and system architecture. For example, STUXNET exploited vulnerabilities in S7 PLCs, Windows operating system, unprotected network paths, lack of detection mechanism etc. As a result, only monitoring devices (such as hardware counters, unusual activities in CPU or unusual events), or network traffic and application level protocol traffic is not sufficient as some of the advanced persistent threats (APTs) camouflage themselves by injecting DLLs in legitimate libraries or applications, by making stealthy attacks which provide no significant sign of unusual activities at the device or network level etc. This necessitates one to monitor the physical dynamics of the various components of the physical system under supervisory control. Therefore, anomaly detection in the physical dynamics at various sensors is employed. However, since physical dynamics of most physical systems – such as power system has a lot of unpredictability and stochastic variation in their dynamics based on generation loss or use of renewable energy sources which are intermittent, loss of load, sudden load encroachment, faults developing suddenly in transmission or distribution lines or in generators etc, anomaly detection is not possible through signature or rule based methods except for drastic anomalies. Especially for stealthy attacks, it is quite challenging. For supervised learning requiring labelled data about physical dynamics is also quite rare – and most data sources are simulated or emulated. Therefore, unsupervised learning methods are often the only way to devise intrusion detection mechanisms based on anomaly detection. In this layer, continuous monitoring, and machine learning based detection of abnormal behavior will be the main thrust of research. This requires expertise in machine learning, domain knowledge in specific critical infrastructure such as power system dynamics, or dynamics of a factory automation, in automotive and UAV control.

This layer research will be led by Prof. Sandeep K. Shukla, along with domain experts – Prof. Saikat Chakraborty for Power System, Prof. Nishchal Verma for Industrial Control System, Prof. A. K. Ghosh for UAV control and dynamics, and Prof. Soumyajit Dey from IIT Kharagpur for Automotive control and dynamics. The foreign collaborators are from UCSD Data Science Institute in University of California, San Diego, New York University-Abu Dhabi, and Tel Aviv University.

The main topics of research in this layer are:

i. Application of Machine Learning for Anomaly Detection based Intrusion Detection
ii. Threat Modelling for Destabilizing Power System Dynamics, Automotive and UAV dynamics
iii. Resilient Control Algorithms for brining system to safe trajectory when destabilized by a cyber attack
iv. Methodology and Tools development for implement IEC 62443 and NIST Cyber Security Framework
v. Building expertise base in Securing Physical Dynamics of CPS systems

4.3.1.3 Vertical Domains of Focus

As discussed before – 3 vertical domains of Cyber Physical System will be our focus.

Critical Infrastructure CPS: The domain of critical infrastructure CPS such as power systems, water treatment plant, industrial control automation etc., are lucrative target for cyber attackers – especially

attackers from nation states, or terrorists – as they can shut down such critical services in a region – leading to huge economic loss.

According to a study released by Sophos – a security company, in 2018, India was the third most prone to cyber-attacks among all countries with 76 % of businesses having been affected in 2018 [0]. According to a report by CISCO India, 15.1 % of the attacks in 2018-19 in India was against the critical infrastructure businesses [2].

It is therefore, very important that a strong research program be carried out in CI-CPS. At IIT Kanpur the already established Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure (C3i Center) has been engaged in this research for the last 4 years. The C3i center already has established India's first industry scale test beds for power system, water treatment plant, Industrial manufacturing automation and already discovered over 15 new vulnerabilities through its VAPT research. C3i center also has developed a number of tools and technologies for detection, and protection of CI-CPS which has been enumerated in the prior work section.

This vertical domain will therefore be led by Prof. Manindra Agrawal and Prof. Sandeep K. Shukla, the joint coordinators of the C3i Center at IIT Kanpur. The major topics of research in this vertical domain are:

Further Test-beds for newer CI-CPS sectors – such as microgrid, telecommunication, Industrial manufacturing, sewage control, IoT based agriculture test-bed, transportation test-bed such as railway signalling etc.

i. Customize the methodology, tools, technology of the 9 horizontal layers for specific domains such a Smart Grid.
ii. Create methodology prescriptions based on IEC 62443 and NIST cyber security Framework
iii. Create methodology, models, and tools for risk assessment and prediction in CI-CPS based on cyber security attack surface
iv. Build assessment and audit capabilities that can be used to train future cyber security auditors of CI-CPS

Automotive CPS Domain: In the automotive CPS domain, there has been recent works discovering security vulnerabilities and demonstrating their consequences in terms of various attack scenarios (for example, false data injection, denial-of-services, replay-attack, stealthy deception attacks etc.) [3,4,5,9,17]. One of the most well-known automotive attacks reported has been based on spoofing Anti-lock Brake (ABS) wheel speed sensor messages [10] and thus disturbing the braking ability of the car. In this attack, the ABS controller performs wrong braking actuation, due to false measurement data which is received due to the attack. Such attack capabilities of compromising the braking performance of an automotive with false data injection about vehicle speed can lead to fatal accidents without the automotive systems being able to detect any attack. Attacks on control area networks which can disconnect Electronic Control Units (ECUs) have been reported in [14]. However, it is infeasible to physically secure every packet transmission between CPS components due to limited communication bandwidth as well as lightweight nature of computing nodes. In the automotive context, this rules out

using heavyweight cryptographic encryption techniques (like RSA, AES) along with MACs for securing all intra-vehicular communication [6]. Also, in recent times vulnerabilities have been reported even in relatively newer in-vehicle communication standards like CAN-FD, TTCAN, and FlexRay etc., [7]. In the future age of autonomous connected vehicles, the security issue of single vehicles become even more important simply because a single compromised vehicle can be used to compromise a vehicle platoon's safety requirements [8].

In regard to the difference automotive attack surfaces and reported attack scenarios, there has been recently reported works on attack detections inside intra-vehicular networks. These techniques can be roughly classified as follows. Intrusion detection techniques for automotive CAN has been reported in [11]. Autosar based primitives for secure onboard communication can also be found in [12]. Distributed security monitoring of automotive tasks has been studied in [15]. Enhancing automotive networks using data layer extensions has been studied in [15]. Techniques for Lightweight Authentication for securing automotive networks have been reported in [14]. Formal techniques like Probabilistic Model Checking has also been applied towards security analysis of automotive architectures [18]. Security aware scheduling and mapping techniques for automotive architectures have been proposed in [19].

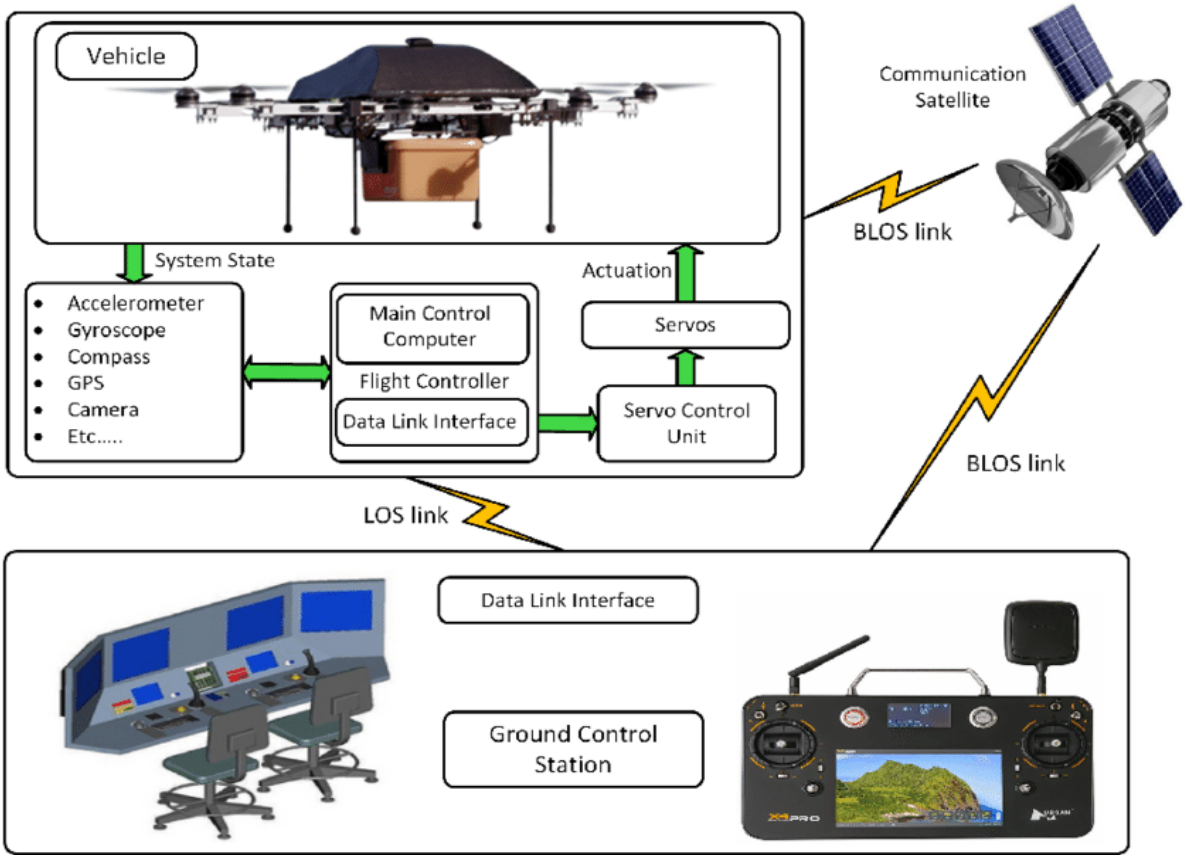
The automotive security work will be led by Prof. Indranil Saha from IIT Kanpur and Prof. Soumyajit Dey from IIT Kharagpur.

The summary of the research problems to be tackled for this domain:

i. Development of Automotive Software Design and Simulation Testbed
ii. Risk Modelling and Analysis framework for Risk – especially due to supply chain dependence and vulnerabilities
iii. Light weight crypto solutions for intra-processor communication over CAN
iv. Redundancy architecture with heterogeneity for risk reduction
v. VAPT methodology and Tools for Automotive Security

Unmanned Vehicle CPS (U-CPS): As can be seen in **Error! Reference source not found.**, – an UAV system architecture contains a large number of sensors, actuators, on-board control as well as ground station based monitoring and control.

Figure 3: UAV System Architecture [20]



These naturally exposes the UAVs to various cyber-attack possibilities. In [20] – a good exposition can be found on how UAVs can be hacked, and UAVs can also be used to breach privacy of people. UAV control has three different types – Remote-pilot Control, Remote-supervised Control, and Full Autonomous Control. IIT Kanpur team has developed UAVs with all 3 types of controls over the last few years. There are 3 major components in the UAV system architecture: on-board flight controller, Ground Control Station, and the Data Links between the ground control, and on-board control, as well as datalink between satellites and the on-board control. The threat models for which we plan to develop mitigation techniques, detection mechanisms of attacks, and response mechanisms can be summarized as follows:

i. Attacks on on-board flight controllers and ground station controllers (malware attacks, exploitations, DDoS attacks, authentication bypass etc.)
ii. Jamming or spoofing of GPS data
iii. Jamming or spoofing of UAV transmissions
iv. Manipulation of captured images and data
v. Injecting falsified sensor data
vi. Malicious hardware/software (Trojans, counterfeits, and side channel-based attacks, unauthenticated patches etc.,)
vii. Attacking the mission assignment system

viii. Man-in-the-Middle attacks on Communication channels (replay attacks, eaves drop etc.)
ix. Denial of Service

As a result, we have to build the following technology solutions

i. Secure boot, intrusion detection, authenticated and authorized access
ii. Light-weight encryption and digital signature mechanisms and corresponding key refreshing mechanism
iii. Malware screening
iv. Detection of Jamming and moving to a robust modulation regime (frequency hopping, or spread spectrum) etc.

The U-CPS vertical will be led by Prof. A. K. Ghosh and Prof. Sandeep Shukla from IIT Kanpur, with collaboration from NYU Abu-Dhabi, Tel Aviv University, and Prof. Vinod Ganapathy from IISc.

4.3.1.4 The Methodology and Research Work to be carried out

4.3.1.4.1 Hardware Layer:

The promises of Cyber Physical Systems can only be realized if security is addressed from its very inception. CPS provides several attack surfaces, side channel analysis being one of them. CPS is instituted of heterogeneous components, typically designed as a network of interacting elements with physical input and output instead of as standalone devices. Security of CPS is often provided by ensuring confidentiality, integrity, and authentication by incorporating cryptographic techniques. However, the implementation of these cryptographic algorithms can itself be targets of further attacks, called side channel analysis. For example, the power consumption or the electromagnetic radiations of a bitcoin wallet can lead to the leakage of its private key, which implies the entire technology built on that is compromised. Likewise, autonomous electric bulbs, which are commercially deployed IoT products have shown to leak via power analysis their secret keys which are used to authenticate any firmware upload. Once it is compromised, the side channel attack can be combined with other attack vectors to make the attacks against IoT or CPS go nuclear!

In another attack surface, many of the products used in IoT or SCADA are being purchased from offshore companies and are being packed in foreign fabs. Particularly for safety-critical infrastructure, there is always a possibility and apprehension that these electronics can be infected by stealthy modifications which are called as Hardware Trojans. Detecting these malicious modifications, which can happen at the IC level or even PCB level, are extremely difficult. Recently it is suspected that a Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip (around 0.2 mm). Some of these chips were built to look like signal conditioning couplers, however they contained memory, networking capability, and enough processing power for launching an attack. These microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards. The tampered motherboards were built into several server machines which were assembled by the company. The sabotaged computers made their ways into datacenters of several companies. Alarmingly, when one of these servers were installed and turned on, the microchip altered the Operating System's core to accept further changes. In order to receive further instructions for attackers these Trojan infected chips could also contact attacker-controlled machines! It is indeed alarming and reinstates that detection and isolation of such malware infected electronics is of paramount importance.

The above discussion leads to the following research questions:

a. How to test the side channel robustness of security products being installed in CPS? Can these tests be performed in a black box or gray box approach?
b. How can we develop a Trojan detection test-bed for CPS and IoT products?

To address the first question above, we need to develop test methodology for side channel leakage. This would involve being able to perform the leakage detections in a black box setting, as many of these designs would be without much details. The approach would be also to develop a reverse engineering know-how, from where we can in the first level do an extent of reverse engineering to comprehend the codebase/design executing in the device. This would be followed by a second level approach of developing black-box test-suites for leakage detections, wrt. power, faults, and so on.

To address the second question, a viable approach would be through imaging-based Trojan/counterfeit detection. For example, to sanitize ICs that we get taped out in offshore fabs, we can try to develop a methodology wherein we can try to obtain back the gds2 (the final format sent to the fab unit) by taking high quality images (using the FIB station at IIT Kharagpur) and comparing with the gds2 actually sent during the design developed in our laboratory. One can try to incorporate Image processing techniques accompanied with suitable data-analysis techniques to make the detection more accurate. However, for PCB level Trojan detections, we need to augment the setup with other instruments for imaging, like X-Ray based devices, which are more appropriate for PCB level detection.

Deliverable from this will be a SCADA/IoT Side Channel Test Lab, Trojan Test Lab. The set up and know-how developed in these labs can be then replicated in government cyber security certification agencies such as STQC. The test service at the TIH can be extended to any cyber security company interested in testing their hardware for security vulnerabilities at the hardware layer. However, the TIH will not have power to issue certificates and such set up must be made available at certification agencies.

4.3.1.4.2 Micro-architecture and Platform Security:

Secure and Holistic Memory Systems

Holistic Secure Memory Hierarchies: State-of-the-art techniques for hardening the memory systems are not holistic. These techniques try to patch one level of memory (for example, Intel SGX secures the data stored in the DRAM but does not take care of caches). We believe hardening techniques, if applied in isolation to specific levels of memory system then it can harm the rest of the memory systems. For example, techniques, when applied to caches can affect information leakage at the DRAM controller and vice versa. Through this proposal, we plan to build systems that can provide interaction between techniques that can prevent timing channels at all levels of the memory system and not limited to a few levels. In the context of cyber-physical systems, a holistic memory system should also interact securely with computing resources like a microprocessor, network processor, or even a microcontroller.

Light-weight Secure Memory Systems: In the context of cyber-physical systems, we may not need to harden the memory systems. The users or the trusted components of computing system can use trusted execution environments (TEEs) for sensitive data and computation, and most often they are light-weight in nature. So instead of hardening the entire memory system, we propose to design, memory systems that can harden the information leakage only for the data/code that is running within an isolated

environment. Some of the examples of isolated environments are Intel SGX, ARM Trust Zone, and AMD's secure memory encryption. Through this proposal, we plan to achieve a good trade-off between security, performance, and the power consumption of a cyber- physical system.

Timing Channel Attack Predictors: State-of-the-art timing channel attack detectors detect attacks after an attacker starts attacking different levels of a system: processor core, caches, and DRAM to name a few. These detectors inform an OS or the next layer in the computing stack. In this proposal, we seek to predict the possibility of attacks through timing channels and inform about the same to an OS or the trusted computing layer, to make the necessary actions (e.g., de-scheduling the attacker).

Methodology: We will be using state-of-the-art microarchitectural simulators to simulate our ideas and effective ideas can be showcased on an FPGA. We will also create tools that can predict timing channel attacks on a real system. These tools will provide different knobs at which timing channel attacks should be predicted.
This layer will be led by Prof. Biswabandan Panda with Prof. Pramod Subramanyan from IITK and Prof. Vinod Ganapathy of IISc. Also, the foreign collaborator will be from New York University.

In Summary, the major issues that will be investigated are:

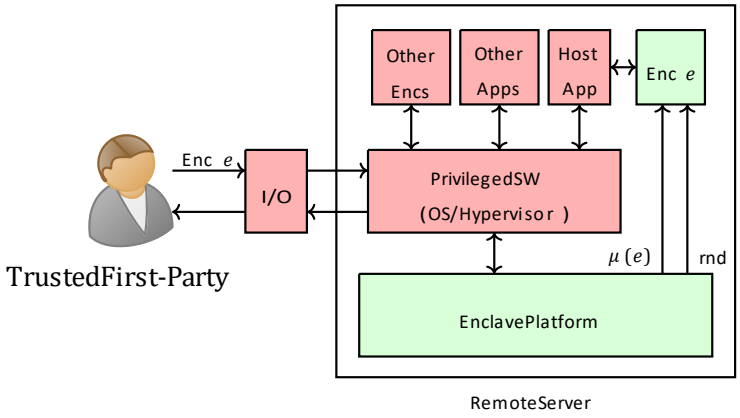
i. Holistic Secure memory design which considers the entire memory hierarchy to avoid the known pitfalls of hierarchy level based secure design
ii. Light-weight secure memory systems for devices such as PLC, RTU etc which does not need memory bound computation but requires to secure information
iii. Timing channel analysis for secure memory systems and rendering them leakage free

4.3.1.4.3 Firmware and Trusted Base, Operating System, and Cloud layers:

On public cloud computing platforms, cloud providers own and administer the system software (e.g., the BIOS, the OS, and/or the hypervisor) that manages the computing infrastructure. A malicious actor can leverage this system software to compromise the integrity and confidentiality of data and code of the clients of public computing infrastructures. Recent hardware advances aim to address this situation by allowing clients to protect their confidentiality and integrity even in the presence of adversarial system software with hardware-rooted guarantees [23, 62, 42, 49, 22, 45].

As an example, the Intel SGX [42, 49, 22], a set of hardware and software extensions that provides support for *enclaves*, which can be used to build a number of novel security applications [28, 52, 24, 43, 56, 60, 69, 47]. SGX hardware ensures that client's code and data in the enclaves are integrity-protected and are opaque to even privileged system software. Thus, from the client's perspective, the Trusted Computing Base (TCB) in the cloud would include *only* the processor, unlike traditional cloud platforms today. The is shown pictorially in Figure 4 **Error! Reference source not found.**. Execution using enclave platforms proceeds as follows: a trusted first-party sends an enclave description (i.e., a binary) to a remote server, which setups the enclave. The first-party then authenticates the enclave using a *measurement [31*] and if the authentication succeeds, the first-party sends the encrypted input to and receives encrypted output from the enclave. Encryption and decryption are only performed within the enclave and the platform's security guarantees attempt to ensure that *all* other software on the remote server are unable to access the enclave's data.

Figure 4: Trusted Execution via Enclaves. Trusted Components in the System are shown in green while untrusted components are in red



A second example that operates in a slightly different threat environment is the Intel MPK, a set of hardware and software extensions that provides support for lightweight user-space isolation. Using the Intel MPK, a user process can create isolated environments even for individual user-level threads. In the case of the Intel MPK, the TCB would include the cloud provider's software as well but would offer clients the ability to create ultra-lightweight isolation, which is of potential interest to emerging microservice-based cloud environments. As software support for cyber-physical systems and critical infrastructure moves to the cloud, it is important to investigate the security of these cloud platforms as well.

The goal of this project is to investigate various techniques to build secure software systems atop such hardware-assisted trusted execution environments. This involves addressing research challenges in (i) making enclave applications and applications that use MPK easier to program, (ii) addressing side-channels in enclave platforms, and (iii) verification of security guarantees of enclave programs. Specifically, we propose to investigate the following research directions.

Programming support for SGX enclaves. A client that wishes to leverage SGX must write its applications to be SGX-aware. An SGX-aware application will place its sensitive data in enclaves and ensure that the code that operates on this data is also placed in the enclave. The SGX hardware places certain restrictions on the kinds of instructions that can execute within enclaves, e.g., system calls cannot be executed within an enclave. Enclave code must be written to respect these restrictions, e.g., by having the application that created the enclave make the system call on behalf of the enclave. The enclave code must also take care to ensure that it does not inadvertently leak sensitive data outside the enclave, and that any sensitive data written outside the enclave is cryptographically-protected using keys stored within the enclave. Thus, while the SGX hardware offers powerful primitives, much of the responsibility of ensuring the confidentiality and integrity of enclave data falls on the application authors.

A number of techniques have been proposed in the literature to allow application authors build secure enclave applications. These techniques range from those that statically verify the absence of information

leaks from enclave applications [65] programming-aids and libraries to allow enclave applications to be written easily with encryption of any egress data being handled by the library [63] and techniques that use programmer annotations on sensitive data structures to automatically split applications into enclave/non-enclave portions [28]. The focus of these techniques is to aid authors of enclave applications, writing *new* code tailored to use the features of the SGX.

The focus of the proposed work will be on frameworks that have been developed to allow *legacy* code (e.g., CPS controllers) to execute within enclaves. While several applications have been tailor-built for enclaves (e.g., [57, 53]), this is a resource-intensive process, and application developers may wish to enjoy the benefits of the SGX without the upfront investment needed to build enclave code from scratch. These frameworks provide the necessary in-enclave support to allow legacy code to operate within the constraints imposed by the enclave programming model, e.g., inability to perform certain operations such as system calls within the enclave. These frameworks broadly follow three different models, as described below.

In the *Library OS model*, an entire library OS executes within the enclave. To port an application within the enclave, the application developer simply loads the application binary, together with any libraries that it uses, and can execute the resulting binary within the enclave. As a result, these techniques can provide *binary compatibility*, i.e., unmodified binaries (or only modified to link with the library OS) can execute within the enclave. Frameworks that implement this model can additionally implement protections against IAGO attacks [34] (e.g., attacks against the enclave application implemented by adversarial system software by tampering with return values) by including a suitable shim (software-hardware interface) layer within the library OS that checks return values. Examples of frameworks that implement this model include Haven [29], Graphene-SGX [70], and SGX-LKL [51].

In the *Library wrapper model*, implemented by Panoply [61] assumes that applications invoke system services via libraries such as the standard C library (libc). Normally, these libraries contain the low-level system calls and other sensitive instructions that cannot be executed within the enclave. Panoply provides library wrappers that enclave-based applications can link against. An application author can use Panoply by simply modifying the code that uses the standard C library to instead use Panoply wrappers, which in turn provides the necessary machinery to cross the enclave boundary.

In the *Instruction wrapper model*, wrappers are provided for the low-level instructions (such as syscall, inb, outb) that are not permitted within enclaves. The wrappers contain the machinery to cross the enclave boundary and take care of data protection—they automatically encrypt all data leaving the enclave boundary and decrypt and ciphertext data received by the enclave.

On the surface, this model may appear conceptually like the library wrapper model; however, the key difference is the *level at which the wrappers are implemented*. Because applications rarely use the low-level instructions such as syscall, inb, outbthat are forbidden for use within the enclave in their raw form, and instead rely on libraries to perform these calls on their behalf, only the libraries that use these calls need to be modified to use the wrappers. The application code that invokes these libraries remains unmodified. SCONE [25] uses this model, however, SCONE is not publicly available, and so in this project,

one of our main contributions will be to develop an open prototype that implements the instruction wrapper model.

We also plan to evaluate the relative merits of the three methods above in porting legacy code to SGX enclaves from a software engineering perspective. For example, some of the criteria on which we wish to evaluate the methods are:

- How much trusted code (in addition to the application's own code) execute within the enclave?
- How much effort is required to port application code to enclaves in each of these methods?
- How much flexibility does each method offer the application developer in engineering the enclave? For example, suppose that the application developer decides to execute some code outside the enclave for performance reasons, how much effort does the developer need to invest to port the code in that way using each of the methods?
- What are the performance overheads imposed by each approach?

Securing SGX from side-channel attacks. While enclave platform hardware ensures that direct access to enclave memory is blocked, a number of side channels [75, 73, 46, 58] can leak confidential information and need to be blocked. Of these, the two most important side-channels that remain only partially addressed in the literature are page tables and transient execution (aka speculation).

SGX relies on system software to manage enclave memory even though the system software cannot access the clear-text contents of these pages. Thus, the OS/hypervisor is responsible for servicing page faults and setting up page table mapping between an application's virtual address and the physical address. Several recent papers have demonstrated that this reliance on system software for managing enclave memory enables *page address-based side-channels* that can leak enclave secrets [75, 73, 74]. The key idea behind these attacks is that it is very often possible to infer properties of the (secret) data processed by an in-enclave victim program by simply observing the page access stream of the enclave. For example, a secret value used in a conditional branch within the enclave may determine the next set of instructions to be executed. If the instructions for the true and false branches lie on different pages, then the page access sequence could reveal some information about the secret being used in the conditional. Previous works have revealed a number of different attack vectors to leak page address streams.

Prior work has demonstrated [75, 74, 73, 40] that adversarial system software can induce page faults any time an enclave program accesses a new page by simply tinkering with the present bit in page table entries (PTEs). Page faults reveal page addresses being accessed by the enclave program to the OS/hypervisor. Researchers have demonstrated an even more powerful attack vector that does not require generating page faults. Instead, adversarial system software can monitor (and periodically reset) the accessed and dirty metadata bits in PTEs to leak victim's page address access stream. Subsequent work showed that even if the system software is not adversarial, translation lookaside buffer (TLB) side channel can leak the page address stream. The attacker co-schedules a thread alongside a victim thread on the same hyperthreaded CPU core. The attacker can then extract the victim's page address stream via a timing attack on the TLB, to which the victim and attacker threads share access.

Unfortunately, previously-proposed defenses for page address-based side channels fall short. They either defend only against a subset of the attack vectors listed above [59, 35, 38, 21] or provide partial support, e.g., by protecting only code pages but not data pages [38]. Some defenses [38, 67] make assumptions that have subsequently been shown to be unrealistic (or broken [59]).

In theory, page address-based side channels can be closed by ensuring *page-access obliviousness* (PAO) [64]. A program that satisfies PAO will always generate the same page access stream, irrespective of the input on which it is executed. Because the page access stream is always the same, no individual execution of the program reveals any information about the secret being processed. However, PAO-based defenses proposed to date place tight restrictions on the programming model of the enclave, e.g., they disallow loops predicated on sensitive values. Consequently, they have only been applied to small benchmarks, and it is likely to add significant performance overhead due to the large number of dummy accesses when applied to larger applications.

We propose to investigate a hardware-software co-designed approaches that provide a practical defense against all known page-address-based attack vectors without introducing runtime performance overheads and without programming restrictions. We propose to defend against page-address based side channels by reducing the resolution of the page access stream and consequently, reducing the effectiveness of the side-channel. We propose to use *large pages* for enclave code and/or data, which vastly reduces the number of distinct page addresses in the stream observable to adversarial system software.

Applications (inside or outside the enclave) use the default page size of 4KB to map virtual addresses to physical addresses in x86-64 based processors, including those from Intel. However, modern processors allow system software the choice of mapping memory at a larger granularity of 2MB or 1GB (called *large pages*) to reduce address translation overheads for applications with large memory footprint [27]. Large pages map significantly larger chunks of the virtual address space e.g., 512× for 2MB pages than with default 4KB pages to reduce address translation overheads. While large pages have traditionally been used for better performance, they can also defeat page-address based attacks. Mapping enclave memory with large pages reduces the resolution of page address stream by at least 512× (262144× for 1GB pages). In our work, we propose to empirically evaluate whether this is typically enough to defeat all known incarnations of page-address based attacks.

A second approach that we will investigate is based on the use of oblivious RAM (ORAM) primitives to secure the page table side-channel in enclaves. Aga and Narayanasamy have recently proposed InvisiPage which has also taken this approach21 by building on Path ORAM. However, our security analysis indicates that InvisiPage is not completely oblivious and leaks some information via *reuse distances*. Our ongoing work indicates that it is possible to provide truly oblivious paging for similar overheads as InvisiPage by building on an optimized variant of the Ring ORAM cryptographic primitive [54]. This proposal will investigate hardware and software optimizations to Ring ORAM to further reduce the overheads of paging. In a second line of attack, we will also investigate *Write-Only ORAMs* [30, 55, 41], which provide obliviousness against a weaker adversary who can only observe write (and not read) operations. In this case, carefully designed lightweight hardware isolation can be used to prevent untrusted software from

observing reads and therefore allow us to use write-only ORAMs which have much lower overheads than read-write ORAMs like Path ORAM and Ring ORAM.

Building secure systems atop the MPK. Unlike the SGX, the MPK works with a different threat model. On the MPK, the underlying operating system and cloud platform is trusted, and the hardware provides primitives that allow for lightweight isolation within an address-space. The MPK has recently been demonstrated to offer very low overheads in large software systems such as web servers, where it is important to isolate the state of one running thread from another [71].

We plan to investigate the use of MPK to build microservice architectures, in particular Function-as-a Service (FaaS) based cloud infrastructures. FaaS is a recent cloud model, as embodied by Apache Open Whisk and Amazon Lambda, that allows for lightweight execution of functions atop the cloud. The client simply specifies a function to execute, and the cloud provider takes care of the rest of the provisioning, and execution of this function atop the cloud. These functions are typically triggered by events and are often stateless and short-lived. As such, they are a perfect fit for the CPS environment where such functions can be used to implement anomaly detection or monitoring services for CPS.

The key problem with FaaS services is that the launch time of these services can often exceed or be comparable to the time to execute the service itself. In this project, we plan to investigate the use of MPK to run FaaS-based services. In particular, we plan to batch requests, and run multiple requests within the same FaaS instance. The issue that arises when requests are batched is that the isolation between requests is compromised. This is where we plan to leverage the features of the Intel MPK, to obtain lightweight isolation between the execution of different instances of the function. Thus, we expect that MPK will allow us to execute multiple instances of the function while just paying the cost of starting up the cloud instance once, thereby amortizing those additional costs.

Security Specification and Verification. An important challenge in the use of trusted hardware platforms is ensuring their security primitives are used *correctly*. Inadvertent programmer errors (aka bugs) can result in confidential information being leaked by the program. To address these errors, this proposal seeks to develop formal modeling, specification and verification techniques for ensuring security of programs that use enclave platforms.

Modeling: Security verification of any system requires modeling adversarial behavior. An adversary model consists of two components: a model of adversarial tampering that captures how untrusted modules can change shared state and an observation function that determines what states are adversary-visible. Tampering captures how the adversary may violate system integrity while the observation function enables reasoning about whether secret information is being leaked to the adversary. The proposal will seek to develop reusable, formally-specified, machine-readable adversary models that can be used to reason about the security of programs relying on enclave platform.

Specification: Once we have a system and adversary model, we need a specification language to formally specify the security properties to be validated. Here, we build on the recent work in hyper properties, specifically HyperLTL [which can be used for specifying security properties like non-interference and

observational determinism [36]. We will investigate two novel ideas over HyperLTL: first-class support for the *tamper* and *observe* functions in the specification language. This allows the adversary model to be parameterized in the property. One can imagine variants of the same program targeted providing different security vs. performance trade-offs for different adversaries. Parameterizing the *tamper* function enables modular specification in such scenarios.

The second novelty is to investigate security-specific classes of hyperproperties. Recent work by one of the co-PIs has introduced security specifications for several important scenarios including security of enclave platforms [68], the first security specification [33] to capture transient execution bugs such as Spectre/Meltdown and Foreshadow [0, 44] and a precise specification of security for authenticated load protocols [50]. Ongoing work is studying quantitative hyperproperties. This proposal will seek to build on this foundation to investigate classes of security specifications that are appropriate for enclave programs specific operating on data gathered from CPS systems.

Verification and Validation: Many security properties are not arbitrary hyper properties, but specifically *k*-safety properties. A few security properties which are not *k*-safety can often be proven using a decomposition to *k*-safety properties. The technique of self-composition [26] can be used to verify *k*-safety properties. Unfortunately, self-composition does not scale to complex systems. While a number of recent efforts have studied techniques for scaling self-composition in the context of model checking, it remains unlikely that any model checking based approach will scale up to the fully automated verification of large software programs. Therefore, this proposal seeks to investigate semi-formal techniques that build on whitebox fuzzing [39] and concolic execution [32], for the verification *k*-safety properties. While fuzzing and concolic execution to find violations of safety properties is well-studied, we are interested in violations of *k*-safety. This will require the development of novel extensions to the fuzzing and concolic execution algorithms. Since these techniques have successfully scaled to the (safety) verification of very large programs, there is reason to be optimistic about their applicability to security verification.

Enhanced Operating System (OS) Security through Attack Surface Minimization

One of the primary challenges to design security hardened OSes using techniques like formal verification is the vast and complex code-base of modern operating systems. Most of the complexity in modern OSes can be attributed to the extensive set of OS APIs exposed through system calls and different administrator configurable elements. An interesting question in this regard, “how many of these APIs are really used in any typical computer system configured with well-known applications?”, when answered can provide possible directions to address many security challenges in the OSes. In this proposal, we want to design a security hardened OS by stripping and/or augmenting the code-base (OS and low-level libraries) based on application platform requirements.

A typical OS caters to the requirements of a variety of platforms by incorporating generic interfaces. For example, the Linux OS (a.k.a Linux kernel) provides a set of generic APIs to meet the requirements of desktops, hand-held devices, real-time computing platforms etc. As a result, a significant number of APIs through system calls and other APIs are rarely used [104]. Therefore, it is perceivable that the most common execution code paths are far less compared to all probable execution paths. Based on this

hypothesis, we propose to perform dynamic execution flow analysis of the Linux kernel and low-level libraries to identify potential dead-code paths and augment the code for a smaller and tractable code-base.

There are several research challenges as described below,

- One of the primary challenges is to determine the run-time execution flow in the presence of asynchronous execution flows. For example, many system calls wait for I/O event notifications which is triggered through external events like interrupts. Therefore, establishing the link between user triggered execution and event triggered execution is non-trivial.
- Building scalable dynamic analysis platforms using common methods like function call profiling may not be suitable for kernel mode execution. Moreover, given the vast code-base and complex code invocations, specialized techniques are required to be designed.
- After identifying commonly used code flows, automated (or semi-automated) techniques to derive equivalent smaller code base is a challenging proposition. This may require adapting specialized compiler techniques like code compaction, equivalence checking, modelling etc.

This research can lead to create an OS distribution with predefined and controlled package management adhering to the minimized OS API support.

So, the main deliverables in these layers are:

i. Development of programming support for correct utilization of Enclave primitives
ii. Development for legacy code porting for enclave platforms
iii. Development of Prototype and implementation of Instruction Wrapper Model
iv. Evaluation of efficiency of library wrapper model vs. instruction wrapper model
v. Methods and tools for side channel analysis and side-channel free implementation using hardware/software co-design
vi. Development of function as service model for cloud applications exploiting the address space isolation primitives available in certain hardware
vii. Development of Models and Methods for Security property specification and Verification for Trusted Computing primitives and discovery of vulnerabilities
viii. Development of a stripped-down secure OS distribution for CPS applications

4.3.1.4.4 Advances in Cryptographic Techniques applicable to CPS:

Cryptography is set to play an increasingly important role in our lives as this century progresses. MPC (Multi-party Computation), the standard bearer and holy-grail problem in Cryptography, permits a collection of data-owners to compute a collaborative result, without any of them gaining any knowledge about the data provided by the other, except what is derivable from the result of the computation. In short, MPC emulates a 'trusted party' for the data-owners, that takes the form of an interactive algorithm to be run amongst the data-owners themselves or amongst a set of hired servers in the outsourced setting. With the promise of confidentiality and transparency together, MPC is all set to turn one of the most impactful technologies of this century by allowing cryptographically secure data analysis over sensitive data and bringing in significant social benefits in contexts where data sharing is constrained or prevented by legal, ethical, or privacy restrictions.

Till date, it has shown demonstrable success in several real-life scenarios, with significant payoff to society. For instance, it has been used: (a) to securely analyze the sensitive salary data of more than 10 million of employees in the Greater Boston Area in order to calculate pay disparity across gender and race [81]; (b) to train a model on private medical data held by several sources to offer best treatment for diseases like HIV, skin cancer, retinopathy [96, 76]; (c) to compute the probability of two satellites colliding in the space for satellites owned by competing countries [94]; (d) to implement secure auction to find a fair price for sugar-beet in Denmark [77]. Another important application of secure computation is found when it is simultaneously required to protect and use a secret data. Often a sensitive secret is split into parts and stored in multiple servers so that the secret is protected from an adversary attacking a quorum of servers. The computation on the shared data can be done via secure computation. The secret data, for instance, can be a secret key for an encryption scheme, and the computation can be the preparation of a ciphertext. The growth of the Internet has triggered tremendous opportunities for secure computation.
In summary, MPC not only makes privacy-preserving collaborative computation on sensitive data a reality, but also removes a single point of attack by allowing for distribution of secrets and computation on the distributed secrets. With a rich career spanning for more than 35 years, MPC has seen monumental progress in recent years both in theory and practical aspects. The intense focus in the past decade brought it closer to practical relevance. To improve its accessibility and scalability, the efficiency study of MPC has taken the center-stage in the past decade. Two of the most important complexity measures dictating the efficiency of MPC protocols are round complexity (the number of sequential communications needed amongst the parties) and communication complexity (the volume of bits needs to be communicated amongst the parties). These directly dictate the latency and bandwidth requirement of an MPC protocol when deployed in real network. The study of round and communication complexity for MPC has been done in various settings based on the type of network (over which the parties relate to each other) and the power of the adversary (that controls the corrupt parties).

The focus of this proposal is to look at the utility of hard-ware token on the efficiency and feasibility of MPC. A fascinating line of work in MPC is to circumvent well-known impossibilities using hardware tokens. In fact, there are fundamental classic infeasibility results that were shown to be circumvented by employing hardware tokens such as the impossibility of fair and robust MPC in the dishonest majority and impossibility of secure computation of general setting [86] that was circumvented in the work of [88] functionalities within the universal composability (UC) framework in presence of dishonest majority in the plain model [83] that was circumvented in [93, 78]. These works demonstrate the power of hardware tokens to break the barriers imposed by these negative results and aid in achieving desirable properties such as fairness and UC-security even in presence of dishonest majority. The works that further the line of work achieving fair and robust MPC in the dishonest majority setting with the aid of tokens are [89, 92]. A non-exhaustive list of works that advance the regime of trusted-setup-free UC-secure MPC protocols in the dishonest majority setting given access to tamper-proof hardware token or physically unclonable functions (PUFs) are [95, 87, 80, 84, 85, 90, 79, 91, 82]

In this proposal, we are interested in investigating the role of a hardware token for fair and robust MPC in the dishonest majority world. A token can be seen as a primitive performing a computation (correctly) modeled by a function. The set of n parties involved in an MPC protocol and having access to a token, can send their inputs to the token and receive their outputs as per the function that the token implements. In the most challenging dishonest majority setting, the adversary can corrupt arbitrary and unrestricted number of parties i.e. it is allowed to corrupt up to n- 1 amongst n parties. The corrupt parties are malicious and can deviate from the protocol arbitrarily from the honest execution. The

security goal of *fairness* ensures that the adversary obtains output if and only if all honest parties do. The property of *robustness* or *guaranteed output delivery* says that any adversarial behavior cannot prevent the honest parties from receiving the output. While these strong goals cannot be achieved in the dishonest majority setting [86], the presence of hardware token is known to circumvent the impossibility. These properties are desirable in real-life owing to limited time and resource availability, as they bind the parties to participate in the computation and thus keep the adversarial behavior in check. Furthermore, lack of such strong guarantees can be detrimental in practice. For instance, in real-time applications such as e-commerce and e-auction, an adversary can always cause an abort if the outcome is not in its favor unless a stronger security notion is ensured. In e-voting, the adversary can abort the computation repeatedly, yet learn the outputs each time and use them to rig the election.

The features of token that we would like to ponder over are:

- **The computing power.** The computing power of the token is an important parameter. The less we demand the better it is. Ideally, the goal is to use a 'small' token with computing power that is polynomial in terms of security parameter. Put differently, it is undesirable for the token to be 'big' and doing computation that is dependent on the circuit size of the function to be computed viaMPC.
- **Trust.** In reality the token will be produced by third-party (potentially malicious) manufacturers. The less the trust we demand from the token the better it is. We consider two trust models– colluding and non-colluding. In the former, the token can collude with the adversary i.e. it shares all the information it receives from the honest parties with the adversary. In the non-colluding setting, it does not collude with the adversary. In both the above setting, we additionally enforce that the token must not learn the input and output of the honest parties in the MPC.
- **No of calls.** The less the number of calls we need to the token to complete MPC the better itis.

Feasibility-wise, we would like to seek what is the minimum that we require from a token in terms of its computing power, trust and number of calls to achieve robust and fair MPC. We would also like to check the interplay of these features such as– (a) does restricting to a single call to the token necessarily require the token to perform computation that is exponential in the security parameter and/or number of parties (or that is function dependent)? Or alternatively, (b) does restricting to a single call to the token necessarily require any MPC protocol to leak the inputs of the honest parties to the token? (c) can we realize MPC with information-theoretic security, without relying on cryptographic assumption, while assuming small tokens and small (say, constant) number of calls to the token? Often, the cryptographic operations leads to loss of efficiency and performance. Therefore, this question is also related to efficiency of MPC. We would also like to see how token can help improve the efficiency of MPC protocols. That is, designing communication and round efficient MPC constructions with the aid of token is yet another goal of this proposal, which remains unattended so far.

Other than the MPC work – in the cryptographic thread, we also want to provide the following deliverables:

i. Development of Hardware token based fair and robust MPC where there is a majority of adversarial node – this is important for a CPS setting where a secret need to be computed to be shared between various components of the system

ii. Development of Lightweight cryptographic algorithms to be used in the real-time communications between sensors, PLCs, SCADA, actuators etc

4.3.1.4.5 Network Layer Security:

Learning to defend against cross-layer attacks:

Although wireless networks are well-known to be vulnerable to a variety of attacks, they continue to be used widely, necessitating the development of efficient and effective defense mechanisms. We consider the design of algorithms to defend against cross-layer attacks, wherein seemingly minor modifications in a single layer result in catastrophic changes in the so-called target layer. A simple example is that of MAC poisoning, wherein attacks at the MAC layer (such as jamming of channel reservation messages) results in making the node unable to discover free channels and ultimately reduction in the throughput. Cross-layer attacks have unique features that obviate traditional threat detection mechanisms. Such attacks [97] make only minor and unnoticeable changes to functions at non-target layers, which are hard to detect. This is because most threat detection mechanisms are tuned to detect large changes and ignore small ones. Bayesian learning has recently been successfully applied to detect and mitigate such attacks. The key idea is to observe the evolution of various metrics at all layers, and then classify if a particular node is under attack. Being the first algorithm for this purpose, many critical aspects such as efficiency and reliability have not been studied.

We propose to study cross-layer attacks in more detail and develop a more efficient and reliable algorithm for the same. By leveraging recent advances in non-parametric learning, we will build scalable algorithms that can carry out the detection and mitigation of attacks over large networks.

Defending against GPS-Spoofing attacks in power systems

Phasor Measurement Units are increasingly being deployed in most smart grids worldwide. Unlike traditional SCADA measurement units, these provide phase information, but at the same time are vulnerable to GPS spoofing attacks. In this setting, an attacker transmits a GPS signal to which the PMU may lock. Subsequently minor changes in the attacker's signals may result in large changes to the system state. If the state is being monitored (either manually or automatically) the subsequent corrective action may de-stabilize the power system. Indeed, systematic attacks at PMUs can have a catastrophic effect on SE and consequently the grid. The authors have already carried out extensive tests on the effect of GPS spoofing at lab-scale [98]. The relevant system being used for testing is shown in Figure 5

The problem of detecting and mitigating GPS spoofing attacks has been investigated from multiple angles. Of interest are approaches utilizing optimization algorithms capable of looking at network-wide PMU data to identify compromised PMUs. Since the overall problem is non-convex, pertinent approaches have sought to solve the joint-state estimation and attack mitigation problem using alternating minimization approach [98]. A key disadvantage of such approaches is the lack of reliability and robustness: they are neither guaranteed to converge nor can handle dynamically changing states. We propose to remedy this problem using online algorithms capable of continuously tracking and processing dynamic PMU data to remove spoofed PMUs and generate clean state estimates.

Airtight Sandboxes for Network Applications

Overview: Proliferation of network applications into end user systems accompanied with rising number of attacks over the network using the network clients as the entry point require specialized defense mechanisms. Traditional defenses like security audits, firewalls, antivirus software, pattern analysis etc. are not enough to bridge all the security holes. Most of the attacks on endpoint client devices (laptops, mobiles etc.) are possible by entering the system through the network and, exploiting existing vulnerability in the system stack or by taking advantage of security non-confirming actions of novice users. We propose a robust system-level isolation mechanism for the network clients to address the security issues in an efficient manner.

Figure 5: Set up to Generate Time Spoofed Signal and Oscilloscope Screenshot

Figure: Set up to generate time spoofed signal

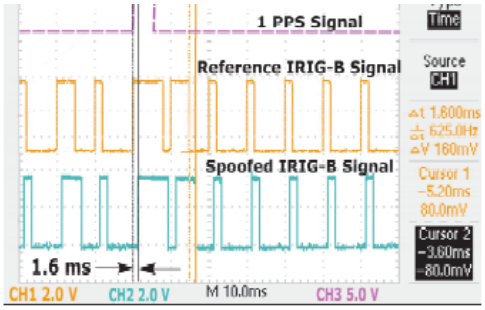


Figure: Oscilloscope screenshots of PPS signal time aligned with reference and spoofed IRIG-B signal to induce error uivalent of 1.6 ms delay.

Detailed problem statement: The malware over network can exploit the software vulnerabilities across all the layers of a system stack---application layer to the firmware/hardware layer. Therefore, application sandbox techniques can not address the security issues presented across the layers. For example, while a browser sandbox helps mitigating attacks through malicious javascripts to a large extent, it cannot protect against a malicious NIC firmware or device driver. We propose to design an OS-level sandbox to isolate the complete network I/O stack from the rest of the system.

There are several research challenges as described below,

- How to isolate different network layers operating at different privilege levels from the rest of the system? For example, a network device driver operates in the kernel space and any user-level isolation cannot prevent the attacks at the device driver layer.
- What are the performance implications of the proposed sandbox? A related question is what are the metrics to quantify security vs. performance tradeoff?
- How securely and efficiently can network applications communicate with the rest of the system? For example, a browser application may want to download a file from the web which requires

interactions with the file system. The proposed system must allow these communications efficiently without compromising security.

4.3.1.4.6 Application Layer:

Application layer has multiple different aspects including malware analysis, memory forensics, honeypots, vulnerability assessment and penetration testing. It also consists of IoT security as most CPS use multiple Industrial IoTs which are distributed and networked.

Development of Security Audit Framework for secure IoT network

Internet of Things (IoT) is a fast-growing network where large numbers of devices are networked to exchange command and control information to coordinate various application level functionalities. It is possible to automate different activities such as a home safety and security, assisted living facility, factory automation, or environment monitoring etc. through an Internet of things enabled distributed networked application. In all such applications, devices need to communicate with each other without human involvement. Even though IoT provides effective methods of creating sensor networks, and applications on top of the network, security and privacy is a major challenge. Mirai bot is one example demonstrating the security loophole in IoT devices. Mirai bot exploited the default authentication credentials of the devices and performed DDoS attack on the Dyn DNS servers. The SHODAN, search engine for the IoT, shows the dark side of connected IoT devices, where several exploitations are possible. The Internet-connected devices, ranging from cameras to industrial controllers, can be compromised according to multiple sources. This may put us on the great risk, for example, hackers can steal credit card numbers, will be able to control our home automation system (home), take the personal medical data, and find where you are and what you are doing. The attacks are due to manufacturing defect (vulnerability) and the end user's ignorance. For example, in Mirai bot, the mistake is from the end user side because the default password was not changed. There are cases, where it is because of manufacturer since they allow low complex password, allowing third party software to automatically install, etc.

Hence, it is necessary to test the security proof of the device before using it. The devices may be of smart home or critical infrastructure, but the attack is a danger to the society or individual even though impact will vary. The challenge with the IoT network devices is the computational capability of the devices and heterogeneity with respect to communication protocols, computational capability, dependency, etc. Considering the growth and need of IoT usage and its security and privacy issues, we plan to set up an IoT security lab with the following objectives.

- To setup the IoT security test bed which will include smart home to critical infrastructure devices.
- To explore the possible vulnerabilities on the IoT devices and suggest a preventive measure.
- To develop a security audit framework for the IoT devices and its communication network.
- To develop a generic secure IoT device communication model which includes lightweight key management, secure channel, etc. for the IoT based smart home and critical infrastructure.

The test bed will include different communication protocol supportive IoT devices to develop a generic security audit framework that can test the data leakage, fingerprinting, etc. The security audit will be on the application as well as the IoT device configuration perspective. Also, the network packets will be utilized for auditing without violating privacy if the packets are captured from the real time application. The test bed will be used to analyze the vulnerabilities of the different types of IoT devices by creating a vulnerability analysis tool which can explore different communication protocols and computationally constrained devices.

4.3.1.5 Security of CI-CPS Plans

4.3.1.5.1 Generic Model of Cyber Physical Systems and Cyber Vulnerabilities

Figure 6 [***99***] shows a schematic model of a cyber-physical system which models the entire physical part of the system as a Physical Plant whose dynamics is modeled with differential equations. The model also contains the interface of this physical system with the digital or cyber part of the system through actuators and sensors. Sensors digitize real-time measurements of analog variables such as current, voltage, pressure, temperature etc., or sense digital data such as switch positions (on or off) etc. These sensor data are communicated to the controllers (which are often distributed through the system because many cyber physical systems are extremely large) over a communication network.

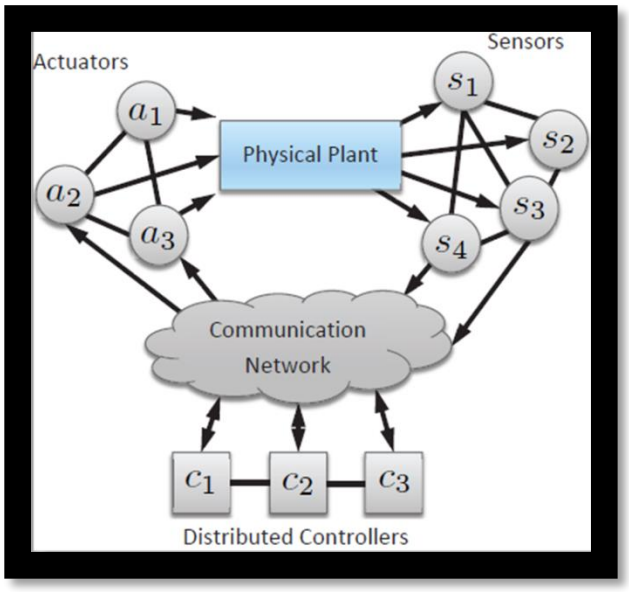
Depending on the system, and owners of the physical assets, and companies in charge of the monitoring and control of these systems, the communication network may have many components – part of which could be wireless (even as simple as low data-rate microwave links or as sophisticated as 3G or LTE wireless network), or wired (all the way from RS-232 to SONET based network). Some companies might have dedicated network (which is expensive) or may have leased lines from telecommunication companies.

Due to IP-convergence, network is often connected to the Enterprise network for business reasons – such as remote monitoring to business policy-based control. This exposes such systems to simple means of cyber-attacks such as Phishing attack where a business person whose desktop is connected to the control network could open an email containing a payload, which can then take over the control of the business network, and in turn the control network. However, since much of the cyber threat models also assume insider knowledge or sabotage, even an isolated control network is not devoid of cyber-attack possibilities. A person with local or remote access to the equipment of the physical plant, or access to the various interfaces such as programmable logic controllers (PLCs) or other Intelligent Electronic Device (IEDs) that are connected to the physical system for measurements and control can exploit vulnerability in these devices to induce an attack on the system. One could also gain access to the control network and create various kinds of man-in-the-middle attacks by either suppressing measurements or control actuation signals, replaying stale measurements or actuation signals, or even injecting maliciously planned false data. These kinds of attacks would then mislead the controllers, and wrong control actions could lead to disastrous industrial accidents. One could also; hack into the controllers or the various other computing elements in the control center such as OPC servers by exploiting vulnerabilities in their design and attack the cyber physical system. In fact, in case of Stuxnet worm, a vulnerability in the Siemens SCADA system was exploited.

In [103*]* an interesting cyber physical system cyber-attack space was conceived which we show in the *Figure 7* , the conceptual attack space is shown. According to Teixeria et.al. [103*]*, there are three dimensions in this attack space: **System Knowledge**, **Disruption Resources**, and **Disclosure resources**. The **System Knowledge** dimension spans from no knowledge of the system architecture, protocols, configuration or components, to full knowledge of the system. The full knowledge of the system is possible for an insider attacker such as a disgruntled employee. The **Disclosure resources** dimension spans from no access to the measurements taken from the physical system in real-time, to full access to all the sensor measurements. The full access is possible if an attacker has broken into the control network and can decrypt any encrypted measurements going form sensors to the control locations. The **Disruption resource** dimension spans

from no ability to disrupt any of the actuation signals, to full access meaning full access to all actuators. The full access is possible, if somehow the attacker can take control of all actuators, or take control of the network, and replace the signals coming from control locations with willfully constructed disruptive signals.

Figure 6: Schematic Model of Cyber Physical System [Source: 99]

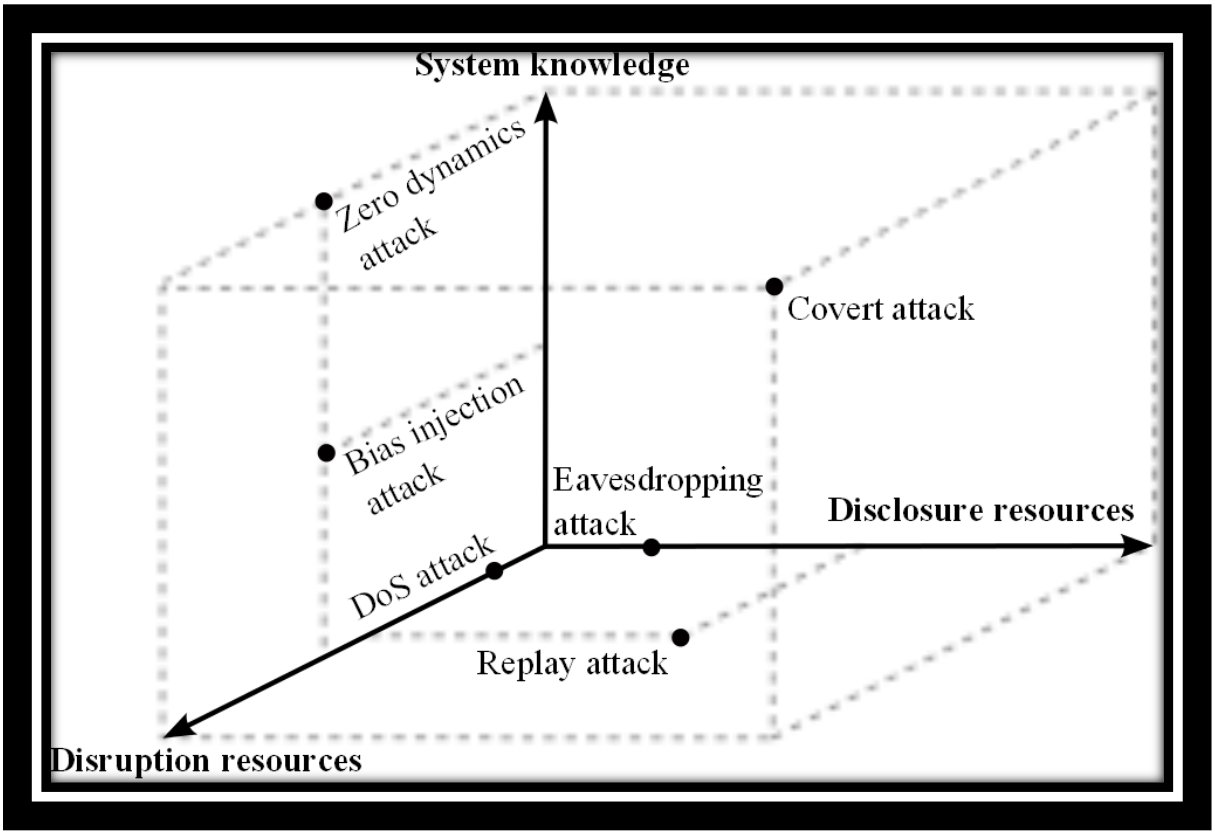


As seen in Figure 7, one can then place various known forms of cyber-attacks on cyber physical systems in this attack space based on what kind of system knowledge, access to network/sensors/actuators the attacker may need to carry out that attack. For example, for Eavesdropping attack whereby an attacker can only read measurements of the physical parameters of the system can be carried out only with partial access to some sensors or some parts of the control network. Replay attack on the other hand requires both partial access to measurements, as well as the ability to change actuation signals for at least some actuators.

Figure 7 provides us with the rationale for the architecture of the SCADA lab we propose to build as part of this project because clearly to study various attacks, we need to construct a lab which has interesting physical system, measurement and actuation devices (such as PLCs, IEDs), RTUs (remote terminal units) that can transform physical measurements to digital data into network packets, protocol converters of various kinds to study various protocols such as Modbus, DNP3, Profibus etc which are used to package and transport such data to control centers or to SCADA Masters, SCADA master servers, HMI displays, and various SCADA software that can process such measurements, display important information, allow the human operators to make control decisions and send back control signals to the field devices. We also need ability to apply machine learning techniques to collected data at the control center, learn optimal control actions or learn how to distinguish between various system states and make decisions, and also ability to induce various attacks on such systems to learn about the security vulnerabilities. We also need to experiment with various methods to enhance cyber security to guard against these various classes of attacks, and experimentally validate the effectiveness of the counter measures.

C3i center at IIT Kanpur already has Power Generation and Synchronization, Power Distribution, and Power Transmission Test-beds, Water Treatment Plant Testbed, Industrial Manufacturing Testbed. We plan to use these test-beds in the research activities of the proposed TIH. However, we also plan to build a few new test-beds in certain other industry verticals.

Figure 7: Cyber Physical System Cyber Attack Space [103]



4.3.1.5.2 National CI-CPS Test Bed for Cyber Security Analysis, Training, and Certification:

The TIH researchers can experiment with various modes of cyber-attacks, and generate data, and develop applications based on formal models, machine learning, stream mining, and other algorithmic techniques to (i) detect anomalies which are symptomatic of on-going cyber-attacks; and (ii) protection techniques to thwart various cyber-attacks. This lab is also meant to help Masters, and Doctoral level students to carry out research in the field of cyber security of critical infrastructures.

In the proposed TIH, we plan to extend the test-bed facilities to address the national need for realistic SCADA test-beds which can be used for (i) cyber security experimentation; (ii) training of personnel; (iii) framing of various protection guidelines for real industries; (iv) demonstration of various cyber threats and mitigation techniques indigenously developed; and (v) for hardware and software in-the-loop testing of vendor equipment to check if they meet security standards, and have plugged all known routes of cyber-attacks. Such a test bed can be a national asset and can be built on the IIT Kanpur Campus provided the institute allows us to build a separate building which will be not only a SCADA test bed, but also house (i) control center for various institutional critical resources such as the institutional micro-grids, chilled-

water plant and its distribution mechanism; water supply system; gas supply system etc; (ii) house a good number of start-ups based on cyber security technologies developed by the researchers at the center, and incubated by the institute and/or the center; (iii) space for vendors to temporarily bring their equipment and software to demonstrate the security of their devices and software by hardware-in-the-loop and software-in-the-loop testing; (iv) facility for NCIIPC personnel to get trained on realistic SCADA test bed; (v) training class rooms, meeting rooms, and offices of some of the engineers, faculty, and students who work on the test bed.

4.3.1.5.3 Research Tasks

In the rest of the section, we provide brief descriptions of some of the problems we want to focus on in the next five years at the proposed TIH. The specific problems are grouped into the seven categories shown in the matrix in the previous section, plus an additional category of Education & Outreach. We believe, some of the problem definitions and scopes would change based on the priorities of the funding entities and their priorities. However, as of now, we list 14 major task areas that we consider would enable the TIH to take off in a major way, and allow the TIH to be the primary destination for students and professionals who want to learn how to secure critical infrastructures from cyber-attacks, as well as to become the main center of research, education, and consulting expertise in India for the cyber security of cyber physical systems.

Analytical Methods

i. Formal Methods based Dynamic Signature Extraction of SCADA Components to Counter Code Replacement Attacks

Simulation/Co-Simulation and Laboratory Emulation

i. Analysis of CPS Threat Models and Discovery of Counter Measures
ii. Discovery and Remediation of Smart Grid Cyber Security
iii. Experimenting with CI-CPS Security Architecture

Cryptography theory and Engineering

i. Cryptographic protocols, Cryptanalysis
ii. Analysis of Side Channel Attacks, and Counter Measures

Software and System Security

i. Automated Protocol Reverse Engineering for Various Protocols and Counter Measures
ii. Cloud Security, Hypervisor Security, Separation Kernel Methods
iii. Perimeter Defense and Penetration Testing

Model Based Analysis

i. Analysis of Enclaves and Trusted Computing Base vulnerabilities and Security Properties
ii. Analysis of Vulnerabilities in Hardware Components such as in PLCs, and IEDs

Machine Learning and Data Analytics

i. Intrusion Detection based on Machine Learning on Physical Dynamics to discover On-going attacks
ii. Application Specific Firewall with Machine Learning

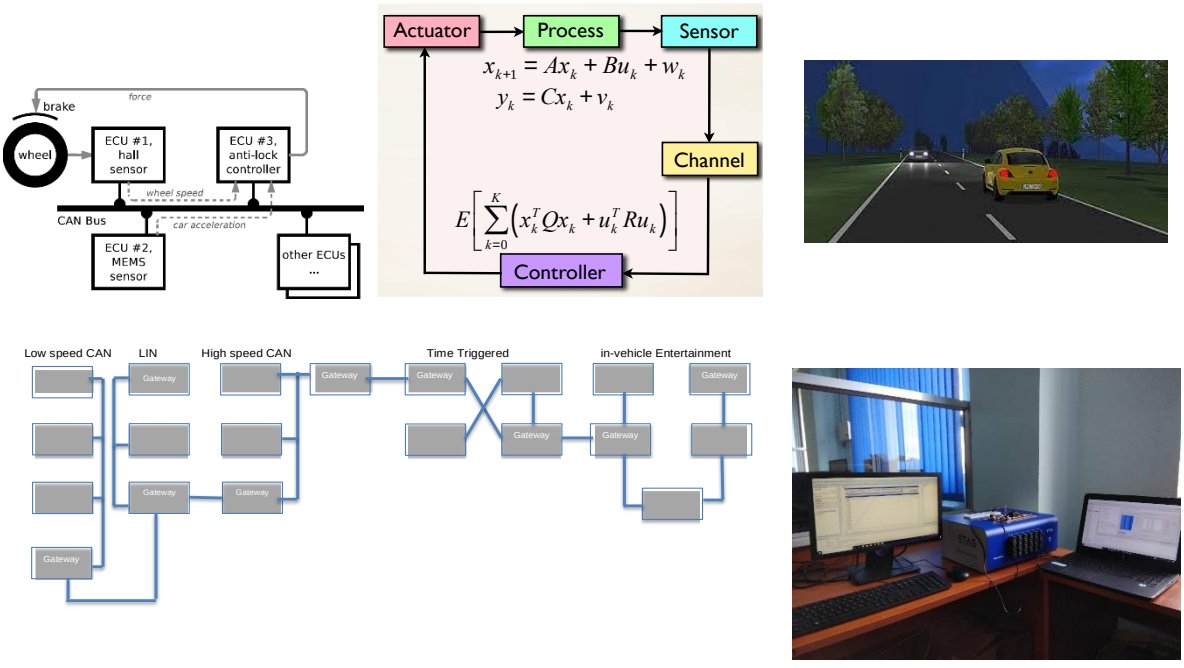
Network Security

i. Intrusion Detection in Control Network using Automated Event Correlation

4.3.1.6 Automotive Security

Unattended communication among devices in distributed CPS implementations makes new pathways for malicious interference. Given that such systems often need to perform safety critical functionalities with real time deadlines within stringent power, energy requirements, the impact of attacks on safety-critical CPS may have catastrophic consequences. Cyber Physical Control systems are an integral part of modern cars having a fair bit of connected electronic components along with mechanical subparts. While such implementations help in creating programmable and connected automobiles, the connectivity aspect among active electronic components and through external gateways make such systems vulnerable to various types of cyber-attacks. Given that automotive software systems often need to perform safety critical functionalities with real time deadlines within stringent resource budgets, the impact of attacks on safety-critical automotive CPS may have catastrophic consequences. With this background we shall like to identify some of the relevant research goals in this domain with suitable motivations drawn from prior art on automotive security.

Figure 8: (Left to Right): Control theoretic vehicle models, Vehicle traffic simulation in a real-time simulation platform, (below) Automotive Networks and their heterogeneity



Research Questions: In this proposal we intent to execute the following research initiatives which in this proposal we intent to execute the following research initiatives which provide CPS researchers some possible handles on the emerging threat of automotive security.

ii. Given that all automotive communications cannot be encrypted due to bandwidth constraints on CAN, what exactly are the high-risk communications and how to implement a sporadic security scheme which does not violate the system safety but helps in maintaining robustness against attacks on CAN bus.
iii. Modern Automotive software stacks come enabled with secure hardware extensions (SHE). However, these measures do not provide robustness against sensor attacks. What kind of hardware/software-based redundancy and monitoring measures can be added into automotive systems so that a significant set of sensor attack scenarios can be mitigated?
iv. Given that deep security vulnerabilities can only be divulged through an automotive hardware test-bed, what should be the best practices for creating a security fault injection setup for such a test-bed. This should further help in in complementing simulation based automotive software and network analysis methods by providing a validation platform for the same.

Automotive Risk Analysis

The proposal is centered around creating a rigorous software engineering methodology and a related test-bed for addressing some of the research questions as mentioned above. Our software methodology considers as input the following items.

A (set of) cyber physical control system models (or their software implementations)

- Control performance criteria of the above systems
- Details about the implementation platform
  - Task maps on ECUs, sampling periods
  - Inter-ECU communication knowhow (bus speed and protocols)
  - Sensor sampling rates, actuation rates
  - Existing Security Countermeasures

With the information tuple as defined above, the objective is to automate the following computations.

a. Identifying the set of sensor inputs having maximum sensitivity to the security and safety violation of the system.
b. Given a set of sensor inputs which are assumed to be under attack, what is the corresponding *risk* of control performance degradation and safety violation. This helps in evolving risk management strategies.
c. Given a platform model with control tasks, what can be a lightweight combination of secure communication strategies (PUF and encryption based) which may be implemented as part of the system in order to mitigate the effect of such attacks.
d. We envisage a tool flow with analysis blocks as shown in Figure 8 which should be useful in this context.

Automotive test-bed for Vehicular safety validation: We need ability to apply machine learning techniques to collected data at the control center, learn optimal control actions or learn how to distinguish between various system states and make decisions, and ability to induce various attacks on such systems to learn about the security vulnerabilities. We also need to experiment with various methods to enhance cyber security to guard against these various classes of attacks, and experimentally validate the effectiveness of the counter measures.

C3i center at IIT Kanpur already has Power Generation and Synchronization, Power Distribution, and Power Transmission Test-beds, Water Treatment Plant Testbed, Industrial Manufacturing Testbed. We plan to use these test-beds in the research activities of the proposed TIH. However, we also plan to build a few new test-beds in certain other industry verticals.

While the earlier procedure is for model based automotive risk analysis and testing, we would like to have hardware-based validation of counter measures as well as a development platform for automotive security analysis. We proposed to design an **Automotive Software Design and Simulation Test-bed** for Autosar based software development, test and validation. The testbed shall have the following features in its **Software component**.

i. Autosar stack for Automotive Software development comprising
    a. Autosar Runtime environment and configuration tools,
    b. Real time operating system with the ISO 26262 ASIL-D safety level and support for the latest versions of the relevant AUTOSAR, OSEK*/VDX and MISRA C standards,
    c. Support for CAN and automotive ethernet, transceivers,
    d. Support for diagnostic tools,
    e. Configuration generator and C code generator
ii. Test and validation of automotive software using real time simulation,
iii. Compatibility with popular autonomous driving simulation tools like Carmaker,
iv. Compatibility with existing laboratory facilities like INCA measurement and calibration tools.

The Setup shown in Figure 8 shall be interfaced with test cars available in IIT Kharagpur for implementing an automotive hardware security analysis setup. The testbed shall be used to implement existing CAN based attacks as well as identify new vulnerabilities possible inside automotive electronic architectures. Possible attack scenarios that we shall start with shall be as follows.

a. **Bus-off attacks** which disconnect vehicle ECUs – we will like evolve control theoretic as well as cryptographic countermeasures against such attacks.
b. **Reproducing other attack scenarios –** ECU re-flash while driving, Noncompliant Access Control, Imperfect Network Segregation etc.
c. **Electrical data forgery** attacks on CAN bus – we will like to implement such attacks and look for possible countermeasures possible in such attack scenarios based on software and fault-tolerance solutions.
d. **Attack surfaces due to connected car features** – we shall incorporate e-sim based interfaces in test car setups and use them for V2V communication, execute spoofing attacks on such interfaces

and identify possible vulnerabilities that may be exploited by online attackers using the such communication links.

e. **Exploit heterogeneity of automotive networks –** Automotive networks are implemented as a mix of different possible vehicular networking technologies like CAN, LIN, MOST etc which interface through ethernet gateways. These different bus protocols often cater to different vehicular control domains like braking, powertrain, telemetry etc. However, the gateways also represent possible vulnerabilities due to interference of packets from different class of traffic flows that they need to handle. We plan to use our testbed to exploit such vulnerabilities and help in evolving suitable countermeasures against them.

Deliverables

i. A software package for
   a. Vulnerability Analysis Tools for Automotive Electronic Architectures
   b. Packet injection on CAN network for attack simulation
   c. Automotive network fault simulation

ii. Synthesis methods for designing schedulable countermeasures – monitoring based as well as cryptographic.

iii. Industry relevant recommendations for Secure Automotive Software Engineering

iv. HW-SW Testbed for Automotive security analysis with consideration for both intra-vehicle as well as inter-vehicle automotive attack surfaces

v. Integration of developed toolsets with the hardware testbed as detailed earlier.

Figure 9: Automotive CPS System Model

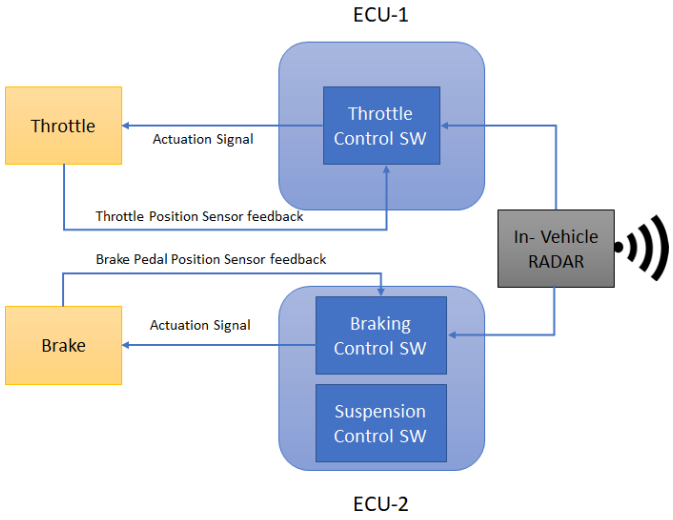
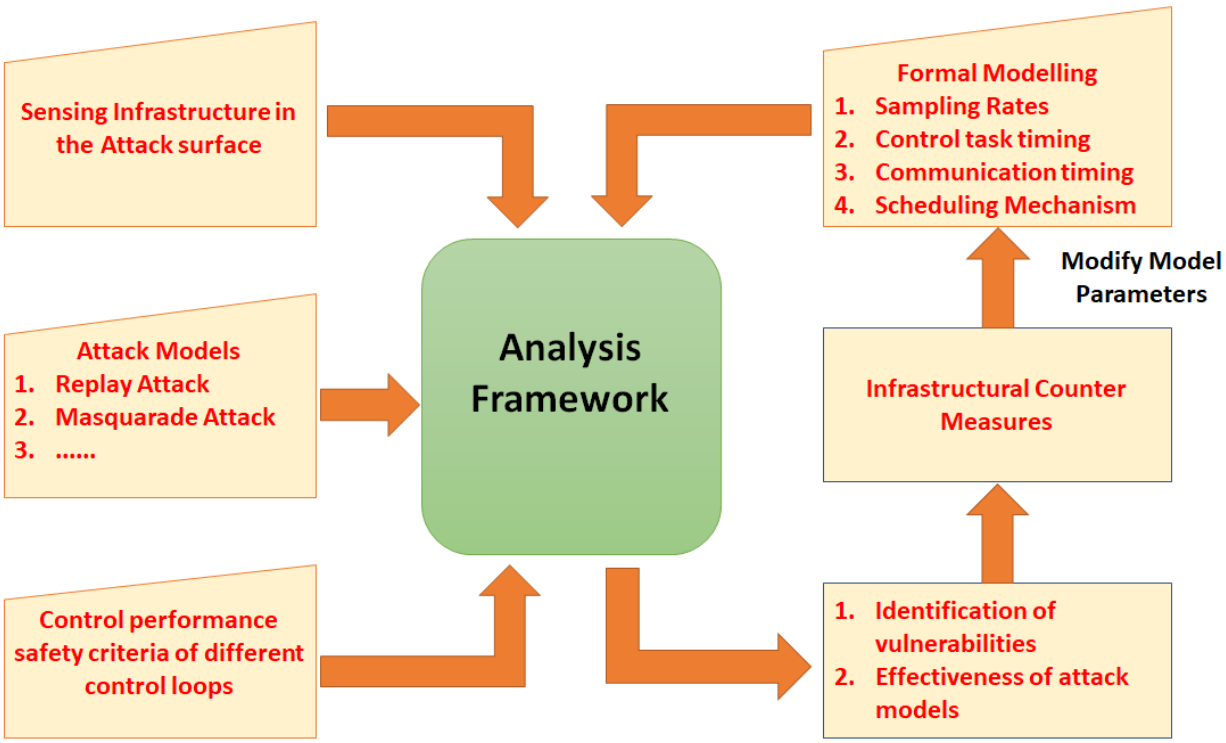


Figure 10: Automotive Security Analysis Framework



4.3.1.7 UAV CPS Security

Unmanned aerial vehicles (UAV) aka Drones are reshaping the next generation of aviation. With significant utility in various use cases by Defence forces, Paramilitary forces, police along with many commercial applications like blood delivery, food delivery, mapping, inspection, etc., Drones are on track to become the next leader in cyber-physical evolution. This demand cutting edge research in every aspect of UAV technology to build the country's self-reliance and to push the technology to new horizons.

With the increasing usage of drones for military and civil applications, the security of drones is getting importance day by day. Regulatory agencies and drone manufacturers are looking for security solutions to track unauthorized drone usage. Security of drone hardware (embedded systems) and Data (wireless transmission) is of utmost importance to regulate drone usage to a wide scale.

Here we summarize the aspects of cybersecurity in the drone industry

Wireless and Data Security

Most commercially available drones are operable through applications that run on a user's phone, tablet or computer. These apps allow the user to manage and pilot the drone and to receive data such as video or images. Drones are also equipped with USB ports that allow the transfer of recorded data. In accordance with the DHS report [104], commercial drones can thus be vulnerable to exploitation since they communicate with their operators using unencrypted means such as radio, WiFi or GPS. This can allow a malicious actor to intercept and review data sent to and from the drone. (It is important to

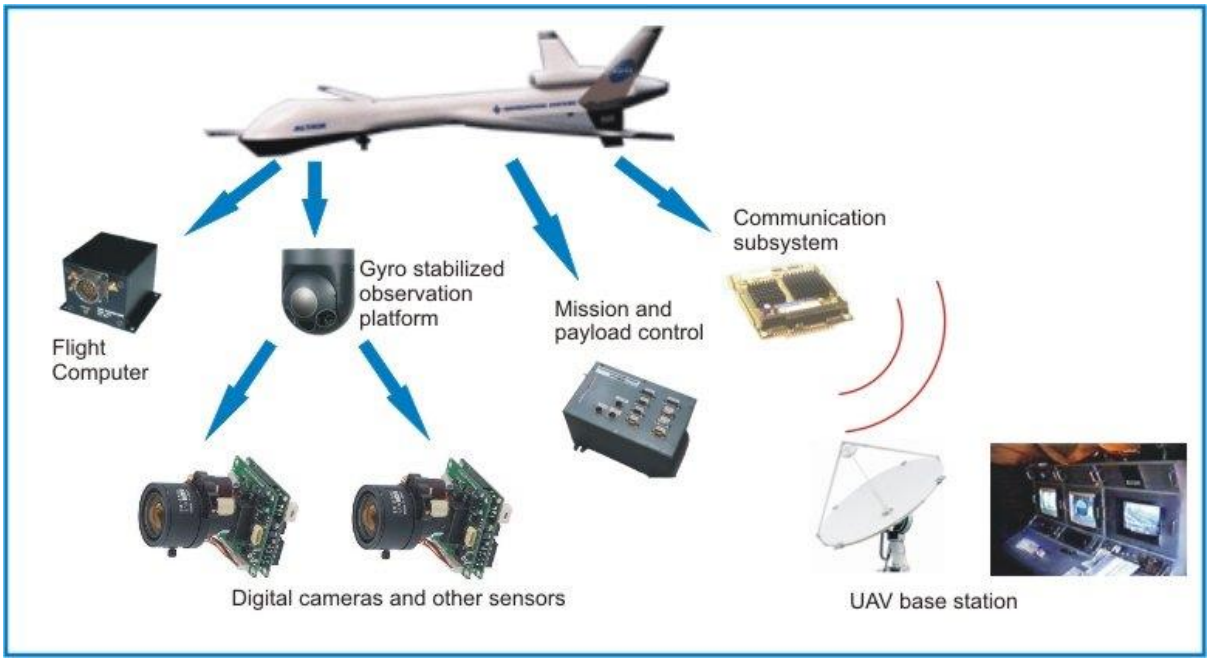
highlight that this is not the case with military-owned drones, where the communication between the ground control and the drone is secured through hardware or software encryption.) Creating reliable architecture and methodology for secure data transmission from the drone is need of an hour.

Embedded Hardware Security and Regulatory authorization

Regulatory agencies such as FAA, EASA, DGCA [106] are actively looking at tamper-proof, hack-proof solutions for drone integration. Flight modules need a standardized architecture for following brief points

i. Verify the authenticity of user/pilot
ii. Validate the flight plan
iii. Integration with existing air-traffic using Unmanned traffic system (UTM)
iv. The secure firmware upgrade mechanism
v. Hardware tamper detection mechanism

Figure 11: (Reference: https://www.researchgate.net/figure/Main-components-of-a-UAV-system_fig1_3278567)



https://www.researchgate.net/figure/Main-components-of-a-UAV-system_fig1_3278567 provides a brief overview of proposed architecture adopted by DGCA in India

Embedded Hardware Security Architecture The Figure 11 briefly provides a generic overview of UAV components. All these components need a security architecture or internal communication as well as external communication to provide authorized access and data security.

Unmanned traffic management system (UTM) Security

With the increasing usage of drones, Unmanned traffic management (UTM) systems are essential for effective management of air traffic. Security of UTM systems and drones play a vital role in restricting unauthorized flights and hack proofing drones.

(Resource: https://securityintelligence.com/using-blockchain-to-address-drone-cybersecurity/)

Figure 12: Unmanned Traffic Management System is required.

Wireless Data transmission Security

Figure 13 provides a brief overview of typical surveillance UAV data. Protecting this data and its secure wireless transmission is a challenging problem statement in drone cybersecurity.

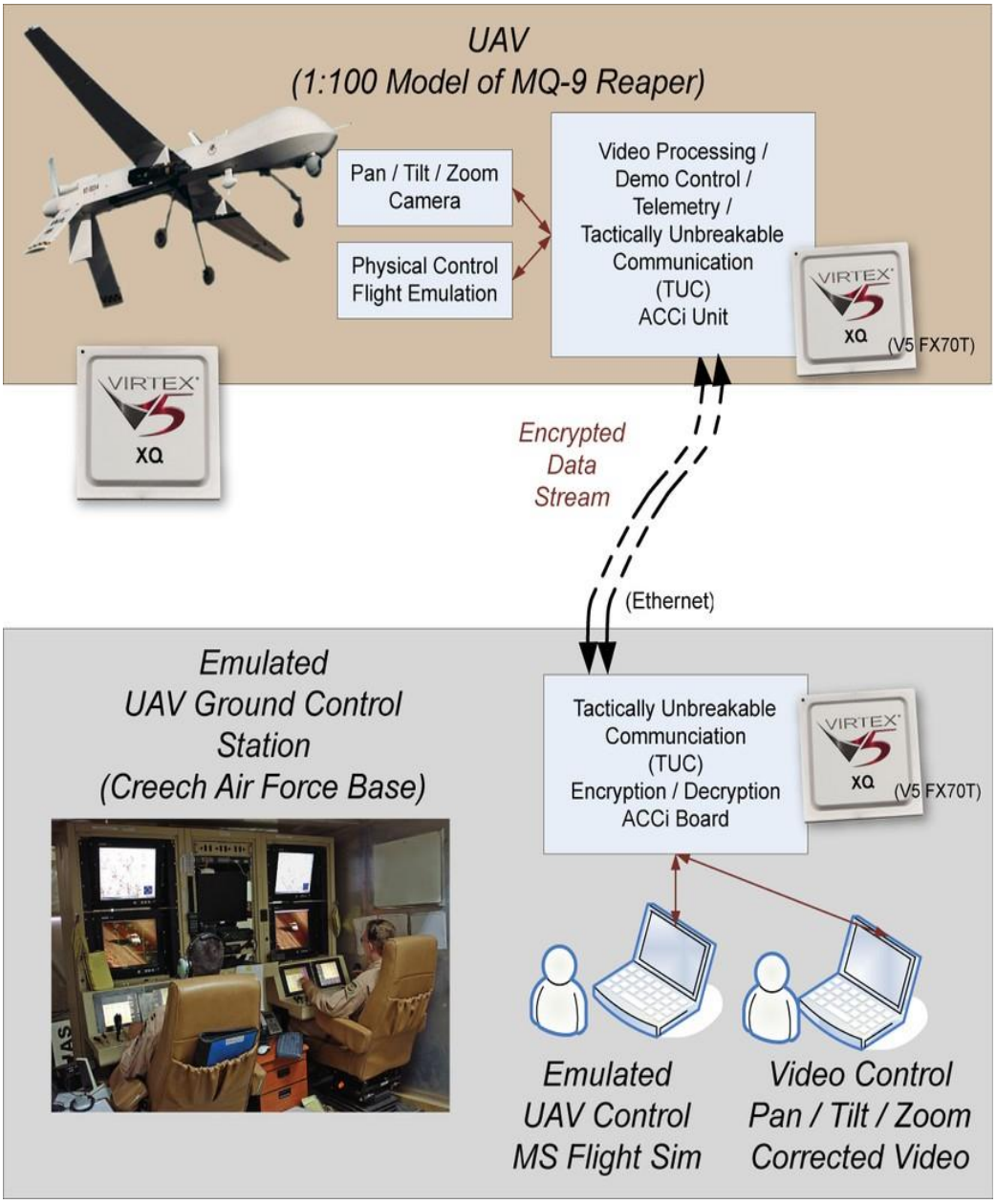
Unmanned aerial vehicles or drones, as their usage grows, are seeing a large number of threat models. This is because not only because drones employed by defense forces can be hijacked by enemy forces by cyber-attacks, but also through cyber attacks one can hijack and repurpose a drone as physical weapons. While the PIs from the Aerospace Engineering department at IIT Kanpur has been building a large number of drones and cooperating with various military and civil administration departments such as the Police, medical supply, and municipalities, it is very important to start working on their cyber security.

Figure 14 summarizes the various areas of cyber security research and development we plan to do in the UAV security arena. The on-board control platform requires strong authentication and access authorization for avoiding any unauthorized software/firmware update on the on-board controller as well as ground control system. To protect one vulnerable software thread not to allow takeover of other threads, software fault isolation is required. Malware analysis and detection and removal is needed as a

service on all processors. Firewall and Intrusion detection system are required. Protection against false data injection during communication between sensors, GPS satellites, ground station and UAV are required. IIT Kanpur will lead this work.

(Reference: http://mil-embedded.com/articles/case-enables-uav-communications-control/)

Figure 13: Data Transmission Security



In the hardware level, light weight and real-time cryptography require implementation in hardware for reduction of latency – which is critical for real-time control loops. IIT Kanpur and IIT Kharagpur will work on this. IIT Kanpur will work on GPS spoofing protection.

The security of supply chain is a critical one as most boards on which control programs are put either for the on-board platform or for the ground control are imported. Therefore, detection of tampered hardware, detection of Trojans is very important. IIT KGP is building a lab for auditing for the presence of these backdoors and for counterfeit hardware and the future UAV components built at IITK will be audited there. Figure 15 summarizes the different augmentations to IITK UAV program and responsible institutes.

Figure 14: UAV Platform Security Components

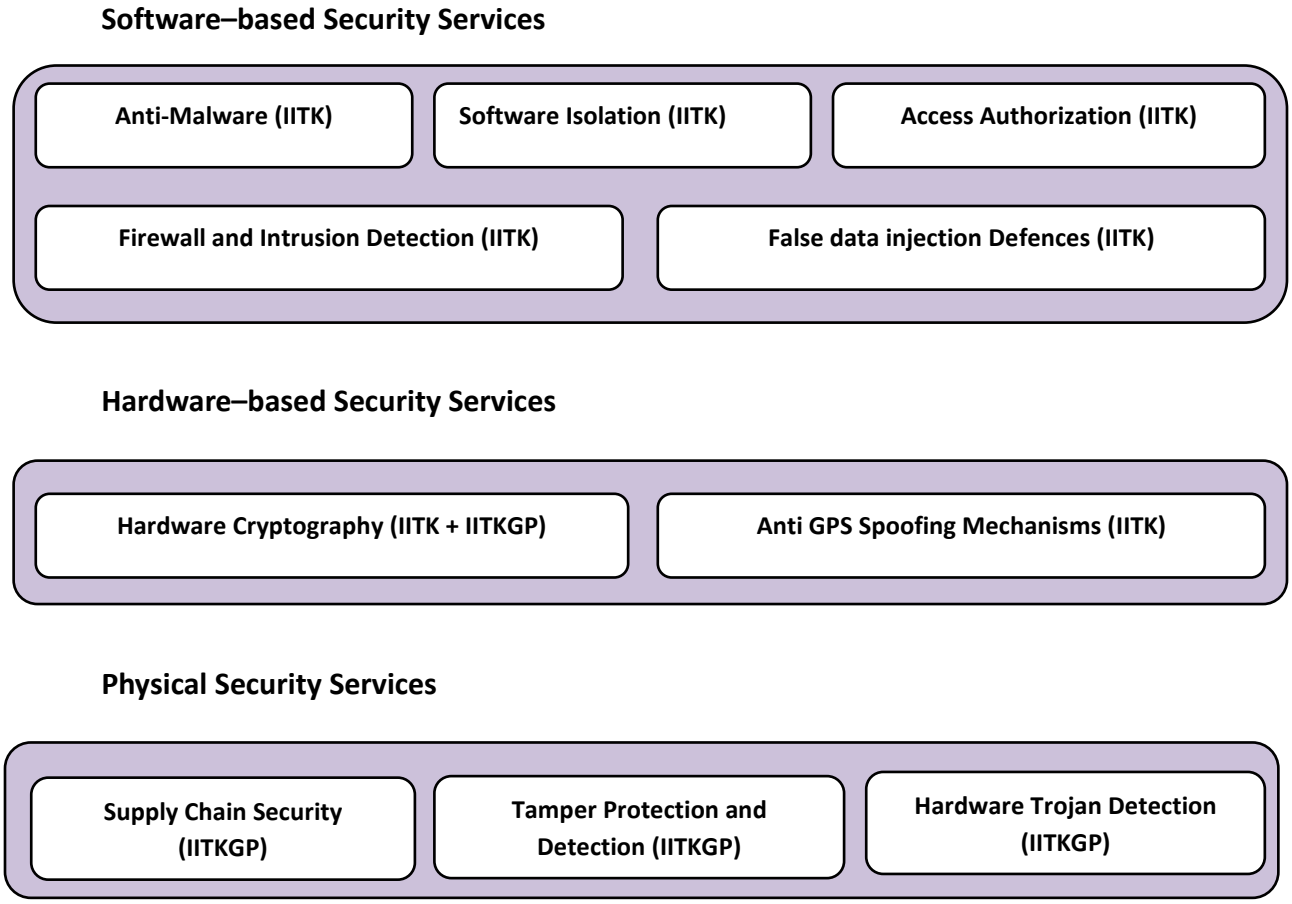
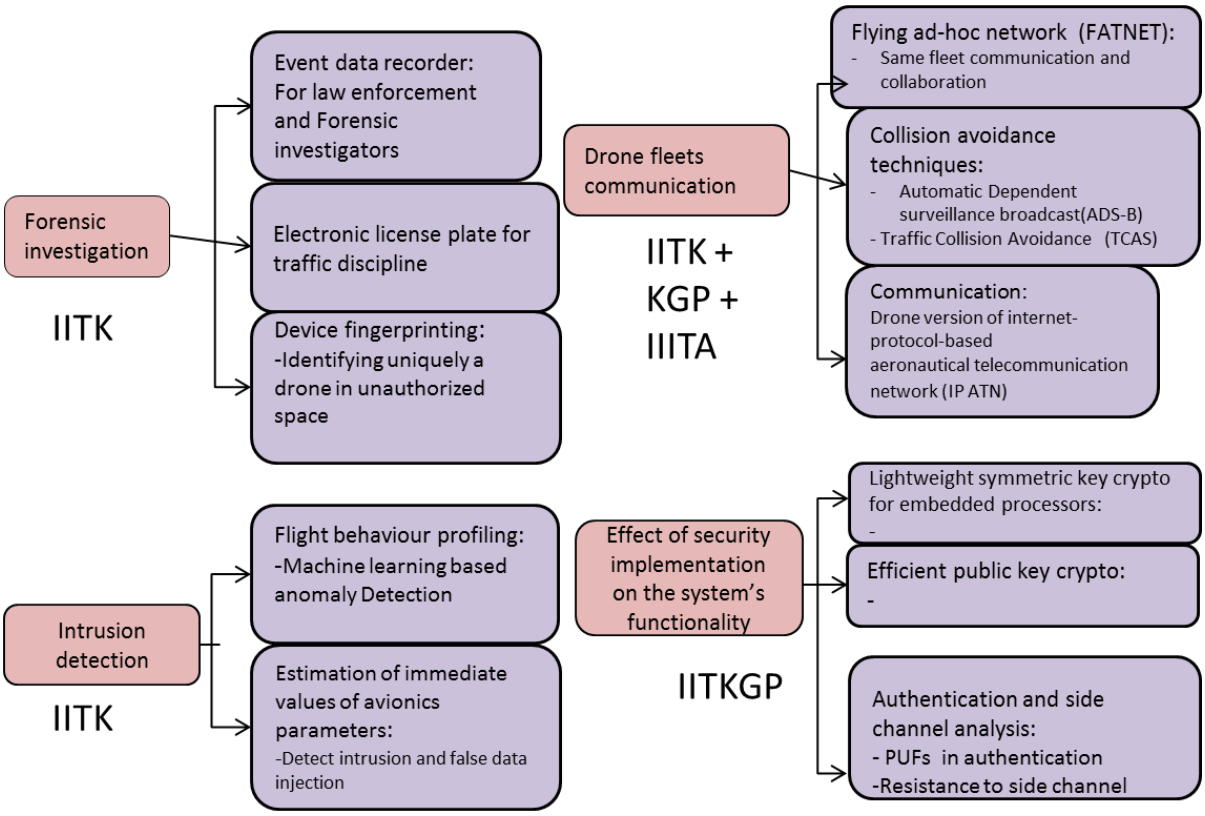


Figure 15: Various use cases for UAV augmentation with forensic and cyber security capabilities



In summary, the work in U-CPS is apply the techniques and tools developed in the 9 layers described in the introduction and suitably customize the techniques for real implementation and create demonstration by inducing various cyber-attacks and the augmented UAV's resistance to those threat models.

4.3.1.8 References:

1. Business Standard, March 13, 2019, "India third most prone to cyber-attacks in 2018 with 76% businesses hit in 2018: Study" - https://www.business-standard.com/article/companies/india-third-most-prone-to-cyber-attacks-with-76-firms-hit-in-2018-study-119031300652_1.html
2. The Hindu, August 18, 2019, "Banking, Government, Critical Infrastructures most targeted by Cyber Criminals: CISCO" - https://www.thehindubusinessline.com/info-tech/banking-government-critical-infrastructure-most-targeted-by-cybercriminals-cisco/article29125650.ece
3. S. Checkoway, D.McCoy, B. Kantor, D.Anderson, H. Shacham, S. Savage, K.Koscher, A.Czeskis, F. Roesner, T. Kohno et al., "Comprehensive experimental analyses of automotive attack surfaces." in USENIX Security Symposium. San Francisco, 2011.

4. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., "Experimental security analysis of a modern automobile," in IEEE Security and Privacy, 2010.
5. Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in CHES, 2013.
6. I. Jovanov and M.Pajic, "Secure state estimation with cumulativemessage authentication," in CDC, 2018.
7. K. T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in SIGSAC. ACM, 2016.
8. Aidin Ferdowsi, Samad Ali, Walid Saad, Narayan B. Mandayam, "Cyber-Physical Security and Safety of Autonomous Connected Vehicles: Optimal Control Meets Multi-Armed Bandit Learning", IEEE Transactions on Communications, Volume: 67, Issue: 10, Oct. 2019.
9. Qirui Zhang, Kun Liu, Yuanqing Xia, Aoyun Ma, "Optimal Stealthy Deception Attack Against Cyber-Physical Systems", IEEE Transactions on Cybernetics (Accepted).
10. Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivasta, "Non-invasive Spoofing Attacks for Anti-lock Braking Systems", CHES 2013.
11. Andrew Tomlinson, Jeremy Bryans, Siraj Ahmed Shaikh, "Towards Viable Intrusion Detection Methods for The Automotive Controller Area Network", CSCS 2018.
12. https://www.eenewsautomotive.com/news/securing-can-communication-efficiently-minimal-system-impact/page/0/1
13. Peter Waszecki, Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Ramesh Karri, and Samarjit Chakraborty,IEEE "IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems", Vol: 36, Issue: 11, Nov. 2017".
14. Kyong-Tak Cho and Kang G. Shin, "Error Handling of In-vehicle Networks Makes Them Vulnerable", CCS 2016.
15. Shanker Shreejith, Suhaib A. Fahmy, "Enhancing Communication on Automotive Networks Using Data Layer Extensions", FPT 2013.
16. Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, Samarjit Chakraborty, "Lightweight Authentication for Secure Automotive Networks", DATE 2015.
17. Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, "Experimental Security Analysis of a Modern Automobile", IEEE SnP 2010.
18. Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, Samarjit Chakraborty, "Security Analysis of Automotive Architectures using Probabilistic Model Checking", DAC 2015.
19. "Security-Aware Design Methodology and Optimization for Automotive Systems", ACM TECS, Vol. 21, No. 1, Article 18, 2015.
20. Riham Altaway and Amir Youssef, "Security Privacy and Safety Aspects of Civilian Drones: A Survey", ACM Transactions on Cyber Physical Systems, Vol 1. No. 2, Article 7, December 2016
21. Aga, S., and Narayanasamy, S. Invisipage: oblivious demand paging for secure enclaves. In *Proceedings of the 46th Annual International Symposium on Computer Architecture* (2019).
22. Anati, I., Gueron, S., Johnson, S. P., and Scarlata, V. R. Innovative technology for CPU based attestation and sealing. In *Workshop on Hardware and Architectural Support for Security and Privacy* (2013).

23. ARM. Security technology building a secure system using TrustZone technology (white paper). *ARM Limited* (2009).

24. Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., Lind, J., Muthukumaran, D., O'Keeffe, D., Stillwell, M., Goltzsche, D., Eyers, D., Kapitza, R., Pietzuch, P., and Fetzer, C. SCONE: Secure Linux containers with Intel SGX. In *ACM/USENIX Symposium on Operating System Design and Implementation* (2016).

25. Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., Lind, J., Muthukumaran, D., O'Keeffe, D., Stillwell, M., Goltzsche, D., Eyers, D., Kapitza, R., Pietzuch, P., and Fetzer, C. SCONE: Secure Linux containers with Intel SGX. In *ACM/USENIX Symposium on Operating System Design and Implementation* (2016).

26. Barthe, G., D'Argenio, P. R., and Rezk, T. Secure information flow by self-composition. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop* (2004), IEEE, pp. 100–114.

27. Basu, A., Gandhi, J., Chang, J., Hill, M., and Swift, M. Efficient virtual memory for big memory servers. In *Proceedings of the 40th Annual International Symposium on Computer Architecture* (New York, NY, USA, 2013), ISCA '13, ACM, pp. 237–248.

28. Baumann, A., Peinado, M., and Hunt, G. Shielding applications from an untrusted cloud with Haven. *ACM Transactions on Computer Systems 33*, 3 (September 2015).

29. Baumann, A., Peinado, M., and Hunt, G. Shielding applications from an untrusted cloud with Haven. *ACM Transactions on Computer Systems 33*, 3 (September 2015).

30. Blass, E.-O., Mayberry, T., Noubir, G., and Onarlioglu, K. Toward robust hidden volumes using write-only oblivious ram. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014), ACM, pp. 203–214.

31. Brickell, E., Camenisch, J., and Chen, L. Direct anonymous attestation. In *Proceedings of the 11th ACM conference on Computer and Communications Security* (2004), ACM, pp. 132–145.

32. Cadar, C., Dunbar, D., and Engler, D. KLEE: Unassisted and Automatic Generation of High coverage Tests for Complex Systems Programs. In *Proceedings of Operating Systems Design and Implementation* (2008).

33. Cheang, K., Rasmussen, C., Seshia, S. A., and Subramanyan, P. A Formal Approach to Secure Speculation. In *IEEE Computer Security Foundations Symposium* (2019).

34. Checkoway, S., and Shacham, H. Iago attacks: Why the system call API is a bad untrusted RPC interface. In *Proceedings of the 2013 International Conference on Architectural Support for Programming Languages and Operating Systems* (2013).

35. Chen, S., Zhang, X., Reiter, M., and Zhang, Y. Detecting privileged side-channel attacks in shielded execution with Deja Vu. In *ACM Asia Conference on Computer and Communications Security (2017)*

36. Clarkson, M. R., and Schneider, F. B. Hyper properties. *Journal of Computer Security 18*, 6 (Sept. 2010), 1157–1210.

37. Finkbeiner, B., Rabe, M. N., and Sanchez, C. Algorithms for Model Checking HyperLTL and HyperCTL*. In Proceedings of the 27th International Conference on Computer Aided Verification (CAV 2015) (July 2015), pp. 30-48

38. Fu, Y., Bauman, E., Quinonez, R., and Lin, Z. SGX-LAPD: Thwarting controlled side-channel attacks via enclave verifiable page faults. In *20th International Symposium on Research in Attacks, Intrusions and Defenses* (2017).

39. Godefroid, P., Levin, M. Y., and Molnar, D. Sage: white box fuzzing for security testing. *Communications of the ACM 55*, 3 (2012), 40–44.

40. Gras, B., Razavi, K., Bos, H., and Giuffrida, C. Translation leak-aside buffer: Defeating cache side-channel protections with TLB attacks. In *USENIX Security Symposium* (2018).

41. Haider, S. K., and van Dijk, M. Flat oram: A simplified write-only oblivious ram construction for secure processors. *Cryptography 3*, 1 (2019), 10.

42. Hoekstra, M., Lal, R., Pappachan, P., Phegade, V., and del Cuvillo, J. Using innovative instructions to create trustworthy software solutions. In *Workshop on Hardware and Architectural Support for Security and Privacy* (2013).

43. Hunt, T., Zhu, Z., Xu, Y., Peter, S., and Witchel, E. Ryoan: A distributed sandbox for untrusted computation on secret data. In *ACM/USENIX Symposium on Operating System Design and Implementation* (2016).

44. Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., et al. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), IEEE, pp. 1–19.

45. Lee, D., Kohlbrenner, D., Shinde, S., Song, D., and Asanovic, K. Keystone: A framework for architecting tees. *CoRR abs/1907.10119* (2019).

46. Lee, S., Shih, M.-W., Gera, P., Kim, T., Kim, H., and Peinado, M. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In *USENIX Symposium USENIX* (2017), pp. 557–574.

47. Lind, J., Priebe, C., Muthukumaran, D., O'Keeffe, D., Aublin, P., Kelbert, F., Reiher, T., Golzsche, D., Eyers, D., Kapitza, R., Fetzer, C., and Pietzuch, P. Glamdring: Automatic application partitioning for Intel SGX. In *USENIX Annual Technical Conference* (2017).

48. Lind, J., Priebe, C., Muthukumaran, D., O'Keeffe, D., Aublin, P.-L., Kelbert, F., Reiher, T., Goltzsche, D., Eyers, D., Kapitza, R., Fetzer, C., and Pietzuch, P. Glamdring: Automatic application partitioning for intel SGX. In *2017 USENIX Annual Technical Conference (USENIX ATC 17)* (Santa Clara, CA, July 2017), USENIX Association, pp. 285–298.

49. McKeen, F., Alexandrovich, I., Berenzon, A., Rozas, C. V., Shafi, H., and V. Shanbhogue, U. R. S. Innovative instructions and software model for isolated execution. In *Workshop on Hardware and Architectural Support for Security and Privacy* (2013).

50. Muduli, S. K., Subramanyan, P., and Ray, S. Verification of Authenticated Firmware Loaders. In *Formal Methods in Computer-Aided Design* (2019).

51. Priebe, C., Muthukumaran, D., Lind, J., Zhu, H., Cui, S., Sartakov, V. A., and Pietzuch, P. Sgx-lkl: Securing the host os interface for trusted execution. In *arXiv:1908.11143* (August 2019).

52. Priebe, C., Vaswani, K., and Costa, M. EnclaveDB: A secure database using SGX. In *IEEE Symposium on Security and Privacy* (2018).

53. Priebe, C., Vaswani, K., and Costa, M. EnclaveDB: A secure database using SGX. In *IEEE Symposium on Security and Privacy* (2018).

54. Ren, L., Fletcher, C., Kwon, A., Stefanov, E., Shi, E., Van Dijk, M., and Devadas, S. Constants Count: Practical Improvements to Oblivious {RAM}. In *USENIX Security Symposium* (2015), pp. 415–430.

55. Roche, D. S., Aviv, A., Choi, S. G., and Mayberry, T. Deterministic, stash-free write-only oram. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017), ACM, pp. 507–521.

56. Schuster, F., Costa, M., Fournet, C., Gkantsidis, C., Peinado, M., Mainar-Ruis, G., and Russinovich, M. VC3: Trustworthy data analytics in the cloud using SGX. In *IEEE Symposium on Security and Privacy* (2015).

57. Schuster, F., Costa, M., Fournet, C., Gkantsidis, C., Peinado, M., Mainar-Ruiz, G., and Russinovich, M. Vc3: Trustworthy data analytics in the cloud using sgx. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy* (Washington, DC, USA, 2015), SP '15, IEEE Computer Society, pp. 38–54.

58. Schwarz, M., Weiser, S., Gruss, D., Maurice, C., and Mangard, S. Malware Guard Extension:Using SGX to Conceal Cache Attacks. *CoRR abs/1702.08719* (2017).

59. Shih, M.-W., Lee, S., Kim, T., and Peinado, M. T-SGX: Eradicating controlled-channel attacks against enclave programs. In *Networked and Distributed Systems Security Symposium* (2017).

60. Shinde, S., Tien, D. L., Tople, S., and Saxena, P. Panoply: Low-TCB Linux applications with SGX enclaves. In *Networked and Distributed Systems Security Symposium* (2017).

61. Shinde, S., Tien, D. L., Tople, S., and Saxena, P. Panoply: Low-TCB Linux applications with SGX enclaves. In *Networked and Distributed Systems Security Symposium* (2017).

62. Shinde, S., Tople, S., Kathayat, D., and Saxena, P. Protecting legacy applications with a purely hardware TCB, 2015. National University of Singapore Technical Report No. NUS-SL-TR-15-01.

63. Sinha, R., Costa, M., Lal, A., Lopes, N., Rajamani, S., Seshia, S., and Vaswani, K. A design and verification methodology for secure isolated regions. In *ACM SIGPLAN Conference on Programming Language Design and Implementation* (2016).

64. Sinha, R., Seshia, S., and Rajamani, S. A compiler and verifier for page access oblivious computation. In *ACM SIGSOFT Symposium on Foundations of Software Engineering* (2017).

65. Sinha, R., Seshia, S., Rajamani, S., and Vaswani, K. Moat: Verifying the confidentiality of enclave programs. In *ACM Conference on Computer and Communications Security* (2015).

66. Stefanov, E., Van Dijk, M., Shi, E., Fletcher, C., Ren, L., X., and Devadas, S. Path ORAM: and extremely simple and oblivious RAM protocol. In Proceedings of the 2013 ACM SIGSAC conference on Computer and Communications Security (2013), ACM, pp, 299-310.

67. Strackx, R., and Piessens, F. The Heisenberg defense: Proactively defending SGX enclaves against page-table-based side-channel attacks, 2017. arxiv:1712.08519v1.

68. Subramanyan, P., Sinha, R., Lebedev, I., Devadas, S., and Seshia, S. A. A formal foundation for secure remote execution of enclaves. In *ACM Conference on Computer and Communications Security* (2017).

69. Tsai, C., Porter, D. E., and Vij, M. Graphene-SGX: A practical library OS for unmodified applications on SGX. In *USENIX Annual Technical Conference* (2017).

70. Tsai, C., Porter, D. E., and Vij, M. Graphene-SGX: A practical library OS for unmodified applications on SGX. In *USENIX Annual Technical Conference* (2017).

71. Vahldiek-Oberwagner, A., Elnikety, E., Duarte, N. O., Sammler, M., Druschel, P., and Garg, D. ERIM: Secure, Efficient In-process Isolation with Protection Keys (MPK). In *USENIX Security Symposium* (2019).

72. Van Bulck, J., Minkin, M., Weisse, O., Genkin, D., Kasikci, B., Piessens, F., Silberstein, M., Wenisch, T. F., Yarom, Y., and Strackx, R. Foreshadow: Extracting the keys to the Intel SGX kingdom with transient out-of-order execution. In *USENIX Security Symposium* (2018), pp. 991– 1008.

73. Van Bulck, J., Weichbrodt, N., Kapitza, R., Piessens, F., and Strackx, R. Telling your secrets without page faults: Stealthy page table-based attacks on enclaved execution. In *USENIX Security Symposium* (2017).

74. Wang, W., Chen, G., Pan, X., Zhang, Y., Wang, X., Bindschaedler, V., Tang, H., and Gunter, C. A. Leaky cauldron on the dark land: Understanding memory side-channel hazards in SGX. In *ACM Conference on Computer and Communications Security* (2017).

75. Xu, Y., Cui, W., and Peinado, M. Controlled channel attacks: Deterministic side-channels for untrusted operating systems. In *IEEE Symposium on Security and Privacy* (2015).

76. [AMS+18] Thomas Attema, Emiliano Mancini, Gabriele Spini, Mark Abspoel, Jan de Gier, Serge Fehr, Thijs Veugen, Maran van Heesch, Daniël Worm, Andrea DeLuca, Ronald Cramer, and Peter M. A. Sloot. A new approach to privacy-preserving clinical decision support systems for HIV treatment. *CoRR*,2018.

77. [BCD+09] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas P.Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael I. Schwartzbach, and Tomas Toft. Secure multiparty computation goes live. In *FC*,2009.

78. [BFSK11] Christina Brzuska, Marc Fischlin, Heike Schröder, and Stefan Katzenbeisser. Physically uncloneable functions in the universal composition framework. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 51–70, 2011.

79. [BJOV18] Saikrishna Badrinarayanan, Abhishek Jain, Rafail Ostrovsky, and Ivan Visconti. Non-interactive secure computation fromone-wayfunctions. In*Advances in Cryptology-ASIACRYPT2018-24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December2-6, 2018, Proceedings, Part III*, pages 118–138,2018.
80. [BKOV17] Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky, and Ivan Visconti. Unconditional uc-secure computation with (stronger-malicious) pufs. In *Advances in Cryptology - EUROCRYPT 2017, 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, pages 382–411, 2017.
81. [BWW] Boston women's workforce councilreport2016. https://www.boston.gov/sites/default/files/bwwc_report_final_january_4_2017.pdf.
82. [CCOV19] Nishanth Chandran, Wutichai Chongchitmate, Rafail Ostrovsky, and Ivan Visconti. Universally composable secure computation with corrupted tokens. In*Advances in Cryptology-CRYPTO2019, 39thAnnual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*, pages 432–461,2019.
83. [CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *Advances in Cryptology - CRYPTO 2001, 21stAnnual International Cryptology Conference, SantaBarbara, California, USA, August19-23 ,2001, Proceedings*, pages 19–40,2001.
84. [CGS08] Nishanth Chandran, Vipul Goyal, and Amit Sahai. New constructions for UC secure computation using tamper-proof hardware. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 545–562, 2008.
85. [CKS+14] Seung Geol Choi, Jonathan Katz, Dominique Schröder, Arkady Yerukhimovich, and Hong-Sheng Zhou. (efficient) universally composable oblivious transfer using a minimal number of stateless tokens. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC2014, SanDiego, CA, USA, February24-26, 2014. Proceedings*, pages 638–662, 2014.
86. [Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In *ACMSTOC*, 1986.
87. [DFK+14] Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and Dominique Schröder. Feasibility and infeasibility of secure computation with malicious pufs. In *Advances in Cryptology-CRYPTO2014, 34thAnnual Cryptology Conference, SantaBarbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, pages405–420, 2014.
88. [FGMO01] Matthias Fitzi, Juan A. Garay, Ueli M. Maurer, and Rafail Ostrovsky. Minimal complete primitives for secure multi- party computation. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 80–100, 2001.
89. [GIM+10] S. Dov Gordon, Yuval Ishai, Tal Moran, Rafail Ostrovsky, and Amit Sahai. On complete primitives for fairness. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, pages 91–108, 2010.
90. [GIS+10] Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay

Wadia. Founding cryptography on tamper-proof hardware tokens. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, pages 308–326, 2010.

91. [HPV16] Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam. Composable security in the tamper-proof hardware model under minimal complexity. In *Theory of Cryptography-14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*, pages 367–399,2016.
92. [IOS12] Yuval Ishai, Rafail Ostrovsky, and Hakan Seyalioglu. Identifying cheaters without an honest majority. In *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings*, pages 21–38,2012.
93. [Kat07] Jonathan Katz. Universally composable multi-party computation using tamper-proof hardware. In *Advances in Cryptology, EUROCRYPT2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*, pages 115–128,2007.
94. [KW15] Liina Kamm and Jan Willemson. Secure floatingpoint arithmetic and private satellite collision analysis. *Int. J.Inf.Sec.*, 14(6):531–548, 2015.
95. [OSVW13] Rafail Ostrovsky, Alessandra Scafuro, Ivan Visconti, and Akshay Wadia. Universally composable secure computation with (malicious) physically uncloneable functions. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 702–718, 2013.
96. [TNO18] Identifying the best HIV treatments with mpc. TNO,2018. https://www.tno.nl/en/tno-insights/articles/identifying-the-best-hiv-treatments-with-mpc/
97. A. Meghwani, J. G. Sreenath, K. Rajawat, S. Chakrabarti, and S. C. Srivastava, "Impact of GPS Spoofing on Synchrophasor Assisted Load Shedding," IEEE PES General Meeting, Portland, OR, USA, Aug. 2018.
98. Risbud, Paresh, Nikolaos Gatsis, and Ahmad Taha. "Vulnerability analysis of smart grids to GPS spoofing." IEEE Transactions on Smart Grid (2018).
99. A. Cardenas, S. Amin, and S. S. Sastry, “Research challenges for the security of control systems”, *Proceedings of the 3rd USENIX Workshop on Hot topics in security*, July 2008.
100. Cardenas, S. Amin, and S. S. Sastry, “Secure control: Towards survivable cyber-physical systems”, *First International Workshop on Cyber-Physical Systems (WCPS2008)*, June 2008.

101. S. Amin, A. Cardenas, and S. S. Sastry, “Safe and secure networked control systems under denial-of-service attacks”, *Hybrid Systems: Computation and Control (HSCC)*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, April 2009, pp. 31–45.

102. A. Cardenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, “Attacks against process control systems: risk assessment, detection, and response”, *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS ’11, New York, NY, USA: ACM, 2011, pp. 355–366.

103. A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, “A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator”, *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 2011.

104. Chia-Che Tsai, Bhushan Jain, Nafees Ahmed Abdul, and Donald E. Porter. 2016. A study of modern Linux API usage and compatibility: what to support when you're supporting. In Proceedings of the Eleventh European Conference on Computer Systems (EuroSys '16). ACM, New York, NY, USA, Article 16, 16 pages. DOI: https://doi.org/10.1145/2901318.2901341
105. DHS report https://www.eisac.com/cartella/Asset/00007102/OCIA%20-%20Cybersecurity%20Risks%20Posed%20by%20Unmanned%20Aircraft%20Systems.pdf?parent=115994
106. DGCA RPAS Manual http://www.dgca.nic.in/rpas/DGCA%20RPAS%20Guidance%20Manual.pdf
107. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/drones-cyber-weapons-reality-not-hyperbole/
108. https://heimdalsecurity.com/blog/cybersecurity-drones/ https://dronelife.com/2019/10/17/drones-and-cybersecurity-an-expert-opinion-on-protecting-industry-against-drone-and-data-attacks/

4.3.2 Supporting Other Institutions

The Hub will provide extensive support to other institutions in the country to develop technologies in the domains outlined above. This will be done through targeted calls for proposals in the first three years and setting aside a minimum of 50% of the funding in technology development for other institutions. As mentioned already, IISc Bangalore, IIT Kharagpur, and IIITA Prayagraj are partnering on some of the aspects and certain amount of funding has been set aside for them in the proposal (see budget section). Once a call is made and selection is done through a committee of experts, the list of engaged institutions should expand significantly.

For technologies developed at other institutions, the incubator at IIT Kanpur (see next section) will also be made available along with necessary support so that these technologies can be brought to the market.

4.3.3 Innovation, Entrepreneurship and Start-up Ecosystem

Startup Incubation and Innovation Center (SIIC, www.siicincubator.com) at IIT Kanpur is a recognized TBI for close to a decade now and responsible for entrepreneurship and innovation ecosystem at IIT Kanpur.

In the past 16 years, since its inception, SIIC has come a long way in developing a robust ecosystem for startups. Leveraging IIT Kanpur's vast infrastructure and elaborate alumni network, hundreds of IPRs, alongside providing meticulous market and investor connects, and utilizing the combined experience, SIIC has a proven record of being a force multiplier like none other, for all our startup incubatees. With our fair share of successful as well as failed incubatee startups, spanning across 2 decades at SIIC, we have developed the experience base and eco-system that become key ingredients in the development of early-stage, technology-focused startups, in areas that are not limited to –

- Supportive and Enabling Community.
- Cohesive Network of Technology and Business Mentors.
- Inter-disciplinary Immersion.
- Access to Growth Capital.
- Strong Operations Support.

From Cyber Security, Flexible Electronics, Aerospace, Defence, Bioscience, Design Innovation, Renewable Energy, Pollution Control, Innovative Waste Management, the best minds of the country tackle some of the most challenging engineering and technology problems at IIT Kanpur. The unique combination of industry knowledge, talent, market concentration, global reach and network of IIT Kanpur ecosystem instils a solution-centric approach among its students, faculty members and researchers.

Alongside our existing innovation ecosystem, the Centre of Excellence would be able to provide the necessary state-of-the-art facilities for product design and prototype-development, research and technology mentoring, including business guidance, training and a much-needed operational support for early-stage startups across technology domains.

Multi-Pronged Outreach for Talent Hunt and Retention

Once the roadmap is aptly laid out for each of the domains, IIT Kanpur shall act as a beacon and use a Multi-Pronged approach to hunt for respective talents/ innovators using a mix of pan-India physical and digital outreach along with mainstream broadcasting. Through nation-wide outreach and rigorous screening, we will ensure that the right talent makes its way to the program. IIT Kanpur through SIIC has been successfully conducting such outreach programs under the BIG program of the Dept. of Bio Technology, Govt. of India and for the INVENT program of DFID UK. This experience gives IIT Kanpur an advantage in terms of the execution of the program. During the first and second year, we plan on conducting 2 outreach events every month (a total of 24 events per year) and 1 event per month in the third year of the program. These outreach events along with social media and physical campaigning shall provide IITK with a steady pipeline of applications from wannabe entrepreneurs and graduating college students.

The value proposition for such talent will have to be a significant factor, in ensuring we get the best of the innovative talent that the country has to offer. To ensure that the program has a long-lasting impact, IIT Kanpur has planned for a lucrative fellowship program with fellowship of up to INR 1 Lakh per month, along with the opportunity for some of the innovators to take ahead their projects as Innovative Startups. We propose awarding up to 200 fellowships to deserving candidates during the project period. IIT Kanpur envisages that the kind of research and development the program entails, would need facilities that the talent can access 24x7 days, any time of the day. Therefore, in the ecosystem that IIT Kanpur builds, every attempt shall be made to institutionalize the talent so that they can maximize their focus over the development work. Hence IIT Kanpur will also provide residential facility of Studio Apartments to accommodate innovators and entrepreneurs involved in the project, within IIT Kanpur facilities as well as the newly developed Noida Outreach Center.

IIT Kanpur through SIIC aims to incubate approximately 50 brightest startup ideas and nurture them through a world-class mentorship program. IIT Kanpur will also provide its Incubation prowess along with appropriate Capital infusion from early stage support to late stage scale up resources for up to Rs. 15 Lakhs outside of their development needs. For this SIIC will not charge any incubation fee, instead it will garner an equity of up to 3%. The benefits that SIIC reaps in future ensures that the entrepreneurs and their success is shared among future entrepreneurs as well, thus making it all a virtuous cycle.

Thus, the innovators will get access to a world-class infrastructure that SIIC plans to build and currently has within IIT Kanpur and its Noida outreach center along with the captive infrastructure of IIT Kanpur which it provides to all incubate companies of SIIC at a rate it is offered to the faculty. In addition, the entrepreneurs will get access to a knowledge base exclusively created for them. The strongest of the value additions SIIC proposes through the program is perhaps the fact that the talent also get a chance to realize their entrepreneurial dreams, further ensuring that the nation's returns are maximized, jobs are created starting immediately, while our Cyber Security ecosystem is strengthened to match global standards.

5 Aims and Objectives

This section lists the development objectives along with outputs/deliverables for each.

5.1 Short and Long-term Research and Translation Goals

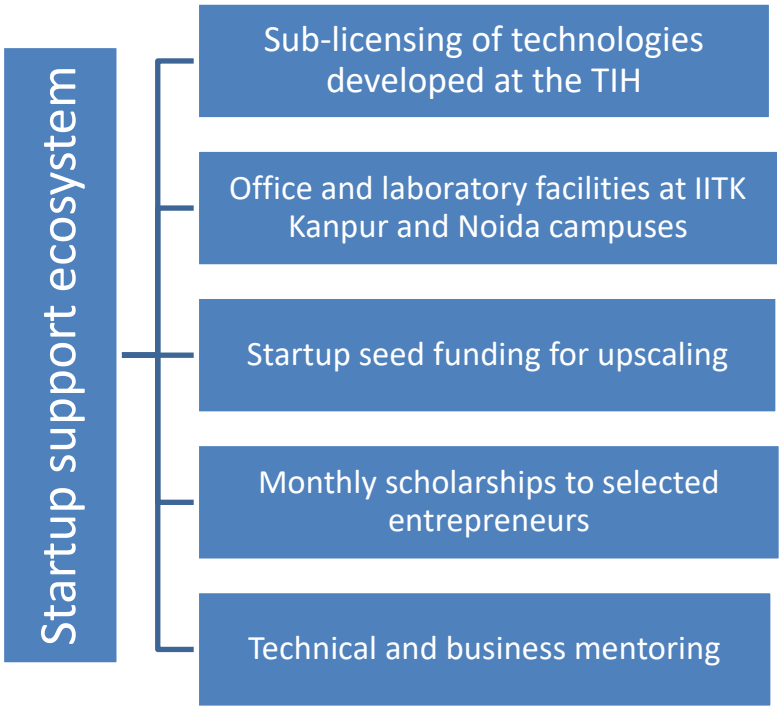
In the short term, the work being done in C3i Hub on security vulnerabilities of critical infrastructure will be expanded to include automotive and UAV sectors. Also, a masters program in cyber security will be launched at IIT Kanpur.

In the long term, (i) hardware testing lab will be created to test presence of trojans and side channels in imported hardware, (ii) work on all nine layers and three sectors will be initiated, (iii) security analysis of model cryptographic algorithms like RSA, ECC, Lattice-based etc will be done with an aim to find weaknesses in them, (iv) at least twenty-five start-ups will be nucleated taking various technologies developed at the Hub to the market, (v) co-development of technologies will be done with at least ten companies in the three sectors, (vi) ten courses on various aspects of cyber security will be developed on online platform and offered as MooCs, (vii) wide range of awareness and executive training programs will be launched along with faculty and student training programs.

5.2 Basic Research

The security of all digital transactions rests on a few key cryptographic primitives, namely, public-key encryption algorithms and digital signature algorithms. These algorithms are primarily RSA and ECC based at present. Both are vulnerable to quantum computers and therefore, there is currently a worldwide contest underway to select an algorithm that is resistant to quantum computers as well. Most of the shortlisted algorithms in this contest are based on integer lattices.

We plan to undertake foundational investigations into the security of all such primitives, with an aim to find weaknesses in them. The chances of success in this are not high given that a large number of researchers have already tried and not succeeded, however, the payoffs of success are immense.



Our edifice of startup support ecosystem shall stand on two fundamental foundations that are required to sustain any incubation program:

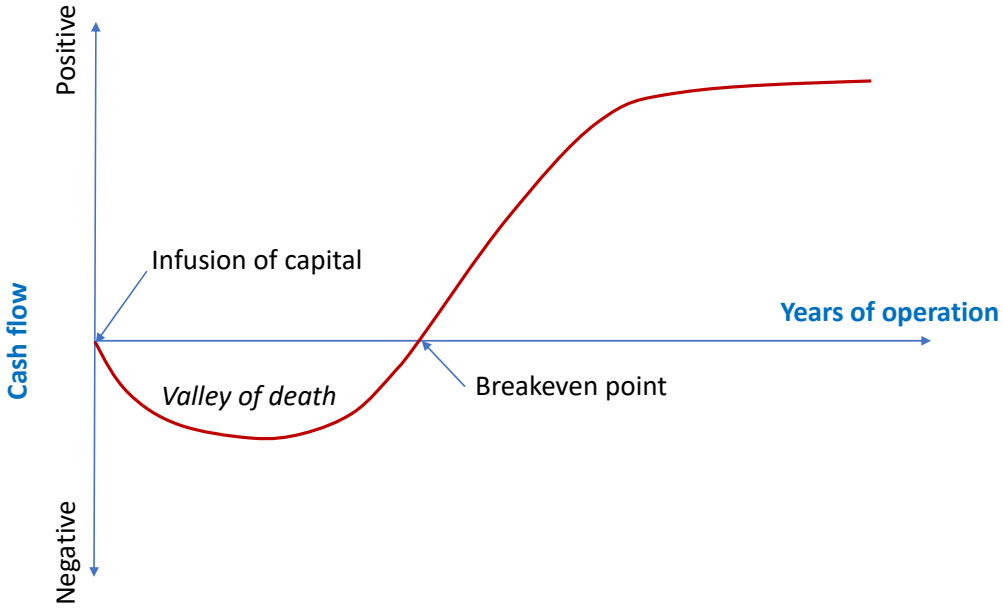
Funding: If we are to attract the best entrepreneurs and innovators to this program, we shall need to heavily incentivize them to join IIT Kanpur as Kanpur does not boast of a strong IT and service sector environment present in other cities like Bangalore, Mumbai and Delhi NCR. Our experience of working with entrepreneurs has taught us that they require support on two levels: personal expenditure and startup seed fund. We would like to offer both these supports to them in this program as described below.

- Every selected entrepreneur shall receive a personal fellowship between Rs 25K to 50K per month for a period of two years, which shall provide for his/her personal expenses. The fellowships shall strictly be non-extendable and non-transferable and only available to up to two founding members of the startup.
- Every startup approved for incubation shall be eligible for a seed funding support of up to Rs. 110 Lakhs (equity/loan/grant or a mix of these) in tranches based on them completing predefined milestones. The equity shall be held by the non-profit company established for running the TIH.

Incubation support: Every entrepreneur needs handholding and peripheral support in his/her quest to becoming the next unicorn. The incubation support plays a pivotal role in providing this support. Entrepreneurs focused on developing their products/services and engaged in business development seldom have the bandwidth to manage legal and accounting side of their startup operations which may pose serious challenges for their scaling up. The incubation support system through their dedicated team

of chartered accountants, company secretaries, lawyers, etc. shall handle these important tasks in the initial phases of incubation.

- Incubation support also involves providing technical and business mentoring to entrepreneurs by a network of experienced business and industry professionals who are well familiar of regular pitfalls for entrepreneurs and help them steer clear of such roadblocks which ensures the startup successfully comes out of the valley of startup deaths.



Thankfully, over the years IIT Kanpur has developed a strong network of startup mentors through its alumni network, industry collaborations and previous incubation programs. These mentors shall provide their support to entrepreneurs on a paid consulting model. TIH shall be responsible for recruiting, compensating and retaining these handpicked mentors for the entire duration of this program. After the 5-year support period, we expect to continue the mentoring program.

5.3 Technology/Product Development

Technology to be developed	The Need	Competitive Advantage	Market Opportunity	Licensing Opportunity	Plan for Commercialization
Industrial Scale Test-Beds for Cyber Security Experimentation **CI-CPS Test-Bed (IITK)**	National Test-beds do not exist – in the US Idaho National Lab, Sandia National Lab, PNNL have Industry scale test-bed for Cyber Security	No such test-beds exist in India at the national scale – our C3i test-beds are already attracted a large number of industries to work	Most industry in the CPS area in India are part of Multi-nationals with few indigenous ones. None have test-beds even like the ones we	Not Applicable	In the TIH – these facilities can be commercialized as testing services

IoT Test-Bed in IIITA **Automotive Security Test-bed at IITKGP** **UAV Test-bed in IITK**	Research. University of Illinois also has a limited scope test-bed. Such a test-bed can be used by Companies to do hardware/software in the loop cyber security testing	with us. Service such as hardware-in-the-loop security testing will also create revenue	now have in C3i and they want to utilize our test-beds for securing their products, or commit to security guarantees to Indian customers		
Side Channel and Trojan Testing Lab at IITKGP	No such lab exists in India – which can be used to audit hardware components such as CPU, PLC, or Routers of questionable provenance to create reports on possible Trojan implantation or Side channel existence	No competitor exists in India and such lab can be replicated elsewhere – providing service of designing and specification of such a lab and methodology of audit could be monetized.	Market is open as of now – for such a service. Supply chain security is a big concern for all critical infrastructures as most devices are imported.	The lab design and methodology can be licensed to others who want to replicate such a lab	It can be that in about 4 years such a lab can monetize testing services, and license their design and methodology of audit
Machine Learning Based Malware Analysis tool	Most anti-malware and anti-virus are signature based – so if a new malware comes into circulation (zero-day malware) – until the signature is updated by the vendor – a machine learning model can detect zero-day attacks unless evasive techniques are implemented but we also have ways to train our models which are robust against evasive attacks	No other Indian company has a tool like this. All anti-virus/anti-malware companies are of foreign origin (Symantec, McCafé, Sophos, Kaspersky etc.,)	If done well (we have developed a large number of models which are published in peer-reviewed international cyber security conferences) the market opportunity is quite huge	Can be licensed to other companies such as Tech Mahindra or BEL for marketable product development	IIT Kanpur C3i Center already plans to commercialize some of the technologies we develop through a startup – so we can do that in this case, but if that does not pan out – Tech Mahindra, BEL and L & T Systems already showed interest in commercializing our technologies – MoUs have been signed with 2 of them
Honeypot Technology for CI-CPS and Dashboard for threat analytics, deployment and monitoring of honeypots	Honeypot technology for web and other IT Technologies are common. However, for Critical Infrastructure automation and control, SCADA monitoring systems, protocol specific honeypots are required. Further, as honeypots are attacked – the threat intelligence collected must be analyzed and data analytics must	There are no Indian company developing CPS honeypot. Smokescreen is the only company that is currently providing IT deception technology and also talking to us in cooperating in the OT honeypot technology space. We also have experience in developing and	As the oil and gas industry, power industry, and industrial factory automation are being targeted increasingly, this technology will become essential – especially if they implement the NIST Framework. There is a wide open market.	We have been talking to two companies who have shown interest in licensing our already existing honeypots we developed and deployed for research. However, once fully developed, the licensing	Multiple companies have shown very high interest in this technology. So the commercialization prospect is great.

	generate actionable intelligence to be acted upon by security engineers.	deploying honeypots for IT as well as OT.		opportunity is very promising.	
Machine learning based Anomaly detection for detecting Intrusion in Cyber Physical Systems	Intrusion detection – signature based, or Machine learning based have been developed in the network traffic analysis and anomaly detection for a while. However, when an attack somehow evades the safe guards of Firewall or an IDS and starts affecting the physical dynamics of the plant under control – the sensor data analysis lead to detection of attacks and such detection can alert the operators of an on-going attack which has passed into the network and started affecting the physical dynamics. Also, localization of the attack can allow quick isolation to save the system.	This technology is at its infancy now – only a few research (Singapore, Israel, and limited in the US) – other than IIT Kanpur C3i Center. So, we have a competitive advantage in having a few approaches already and having implemented them, we are able to detect anomalies. We must leverage this unique expertise and productize and do further research.	One of the major function in the NIST CSF is "Detection" of ongoing attacks. Normally IDS available in the market are host based or network based but only tries to detect activities in the host or in the network – but if they fail to detect stealthy and evasive methods or insider attacks – detecting on-going attacks from anomaly detection is a must. As more critical infrastructure companies implement NIST framework, these tools will be in demand.	If the TIH does not market the tools in this technology via start-ups, companies such as Tech Mahindra, L&T Systems already has shown interest in licensing.	Either through startup ecosystem created for the TIH – the tool can be commercialized or through licensing via some of the collaborator industries – specifically Tech Mahindra, and L & T Systems.
Cyber Asset Management Framework, and Console	One of the major functions of NIST Cyber Security Framework is "Identify" – identifying the cyber assets in an infrastructure, prioritizing them based on their criticality, having the ability to patch them – with authenticated patch, and also alerting the security engineers of the newly disclosed vulnerabilities in these assets – are all part of the "identify" function. We found that many utilities do not have a proper automation to keep	There are some foreign products on cyber asset management but there is no indigenous product. Also existing products do not have all the functionalities we conceive of. Some utilities design in-house databases and through screen design – some visibility into cyber assets but does not have facility to alert on newly discovered vulnerabilities, manage patching through the console, and	To implement NIST framework, this is an essential tool for critical infrastructure operators. So the market opportunity is quite large.	If not productized directly by the TIH, the technology may be licensed for other companies to offer products based on our technology and methodology.	Either through startup ecosystem created for the TIH – the tool can be commercialized or through licensing via some of the collaborator industries – specifically Tech Mahindra, and L & T Systems.

	track of the cyber assets, new vulnerabilities, the patch levels, firmware versions, and no single console to apply patches etc. This requires a software-based system that can in real-time monitor the cyber assets and generate alert based on recently disclosed advisories from NVD database, and provide analytics on the overall cyber asset health and requirements for upgradation, schedule maintenance for patching etc.	provide analytics on overall health indicators.			
Secure Operating System Distribution	One of the major issues with OS such as Linux is that it has a lot of customization and they expose a lot of redundant APIs which result insecure system call paths. One of the goals of the Operating system layer security work in this project is to create a stripped-down O/S based on the needs of a CPS application along with secure trusted computing base – secured through the research at the TIH. This will be very useful for critical infrastructure sector	Other than CDAC BOSS operating system which is based on an older version of Linux Kernel – and hence have vulnerabilities – there is no commercial Indian security hardened OS. So if proven reliable after rigorous testing – and validation – it will definitely provide competitive edge.	In defense sector, as well as CI-CPS sector – there is a potential for market. In the automotive and avionics, certifications of air worthiness will be required and for that common criteria security evaluation will be required.	If successful – may be widely licensed for derivative OS versions	Either through startup ecosystem created for the TiH – the tool can be commercialized or through licensing via some of the collaborator industries – specifically Tech Mahindra, and L & T Systems.

These are some of the products that we have enough preliminary research on – and can confidently predict that productization will be possible. However, as the TIH grows, and various other layers are tackled in research and development, we expect more productization ideas and opportunities to come up.

5.4 HRD and Skill Development

5.4.1 Faculty Chairs in Cyber Security

At present, there is a serious shortage of experts in cyber security domain in the country. While there are a good number of cryptographers, the other aspects of cyber security have few experts. This is evidenced by the fact that almost no top institution in the country is able to offer a high-level program, e.g. masters, in cyber security. It would be critical to bring in more experts in order to realize full potential of the proposed Hub. Therefore, we propose to institute ten faculty chairs and twenty young faculty fellowships in cyber security at various institutions across the country with the aim of using these to attract experts to join the activities of the Hub, especially from outside India.

5.4.2 Development of Cyber Security Curriculum and Outreach educational activities

Courses and projects at IITK and other institutions around India can benefit from the pedagogical aspect of this project. The current sequence of courses in security in most institutes except for IIT Kanpur, do not go into Industrial Control Systems security. Most security courses teach cryptography, hardware for crypto, network security, wireless security, etc. At IIT Kanpur, we have the following series of courses:

i. Modern Cryptography
ii. IoT system Design
iii. Embedded and Cyber Physical Systems
iv. Computer System Security
v. Cyber Security of Critical Infrastructures
vi. Secure Memory Systems
vii. Designing Verifiably Secure Systems
viii. Malware Analysis and Intrusion Detection
ix. Blockchain Technology and Applications

All these courses are taught at the graduate level with a mix of students from undergraduate and graduate population.

IIT Kanpur has currently proposed a new MTech and new M. S by research program in “Cyber Security” – which will be targeted for imparting cyber security knowledge and expertise to students and create man power in cyber security.

Our “Computer Systems Security” course is also available online through ICT Academy program from IIT Kanpur at https://ict.iitk.ac.in/product/computer-system-security/. This online course is currently being used by the Abdul Kalam University of Technology (AKTU) in their curriculum where the online video and media content are available through the ICT academy, and examination is set by the ICT academy for the entire university.

A course in “Blockchain Technology and Applications” is going to be offered via NPTEL on the Swayam platform from January 2020. https://swayam.gov.in/nd1_noc20_cs01/preview is the URL for this course.

IIT Kanpur also plans to introduce an eMasters program in Cyber Security which will consist of 6 courses from the above-mentioned list and may be augmented with other courses.

As a result of all these activities, we believe that if the Technology Innovation Hub (TIH) in Cyber Security of Cyber Physical Systems become functional, not only the students enrolled in degree programs at IIT Kanpur, but also all the start up and industrial partner employees will be able to enhance their knowledge and skill set with the online contents of the various courses in cyber security that we have created.

Further, as outreach activity of the TIH, our curriculum, course content can be further shared with various institutes around India to enhance the manpower in cyber security – especially in the critical infrastructure sector.

IIT Kanpur's C3i Lab (National Interdisciplinary Center for Cyber Security and Cyber Defense of Critical Infrastructure) – https://security.cse.iitk.ac.in has recently launched an executive education program in Cyber Security and Cyber Defense. IIT Kanpur, in association with TalentSprint has designed an Advanced Certification Program in Cyber Security and Cyber Defense for current and aspiring professionals who are keen to explore and exploit the latest trends in Cyber Security Technologies. A combination of deep academic rigor and intense practical approach will allow participants to master in-demand skills and build world class expertise.

As the technology innovation hub will enable us to hire more researchers, engineers, faculty, postdoctoral fellows, visiting faculty – we believe further such programs targeted not only for executives in IT companies, but also utility engineers, and government/defense sector can be launched.

5.4.3 Development of Cyber Defense Skill set among Critical Infrastructure Sector Employees

C3i Center at IIT Kanpur has established India's first cyber physical critical infrastructure test-beds for cyber security research. C3i center has Power Generation, Synchronization, Power Transmission, and Power distribution test-beds. We also developed a multi-stage water treatment plant test-bed, an industrial manufacturing test-bed, and plan to create test-beds for other critical infrastructure under the TIH project. All these test-beds are industrial scale which utilize equipment from all available OEM equipment such as Siemens, Schneider, Rockwell, Wago etc. SCADA systems, PLC based control, DCS based control, RTUs, protocol switches for various industrial protocols are used in these test-beds allowing us to do extensive vulnerability assessment and penetration testing (VAPT) . C3i lab so far has done more than 15 responsible disclosures. Eight CVE (Computer Vulnerabilities and Exploits) have already been credited at the International databases that enlists newly discovered vulnerabilities in computer equipment. Some of the vulnerabilities disclosed by C3i are of severity score 9.8 (severe) to 8.8 (severe), 7.5 (High) and 6.5 (medium).

Under the TIH project, we will have more researchers to enhance our VAPT activities, and develop tools that would allow engineers to discover vulnerabilities much more easily than the manual methods normally used to do reverse engineering and various manual experiments to discover those.

As a result, our center attracts a lot of utilities, OEMs, and government agencies who want to learn the VAPT skill and want to apply them at scale.

We believe that the researchers, engineers and faculty working in the TIH will broaden the base of people skilled in VAPT in India. We also can create specialized training programs for utility sector so we can impart the knowledge to engineers working in critical infrastructure sector.

Another aspect of our work in the C3i which will be further enhanced in the TIH is the capabilities in creating cyber security research oriented test-beds for various industry verticals. We have in the past discussed with replication of such test-beds at other locations such as other IITs, some industry, and even at the government agencies which are concerned with critical infrastructure security.

We believe one of our goal in the TIH will be to train engineers and researchers at other organizations in building such test-beds and also to teach them how to utilize them in various cyber threat modeling, VAPT, and protection/mitigation techniques.

5.4.4 Short Term Courses for Executives and Engineers, Summer Courses, Workshops, and Public Awareness & Education

We consider it as our responsibility as a TIH in cyber security at a premier Indian institute of National Importance to educate and sensitize public on cyber security issues in general.

Given the importance of various critical infrastructures to the national economic growth, and sustained infrastructural growth, it is very important that the critical infrastructure created by the government or private industry is safe from cyber-attacks. We already established the fact that today's smart infrastructures are connected to the Internet through various IP-convergence modes due to business and pragmatic reasons, cyber-attacks on such infrastructures are imminent threats. India needs a trained work force that has good knowledge of various techniques of cyber-security – not only in the areas of encryption, authentication, and perimeter defense through firewalls etc. Especially, we have shown that the cyber security of cyber physical system requires a highly integrated interdisciplinary knowledge, and techniques borrowed from game theory, machine learning, stream mining, complexity analysis, program analysis etc., along with domain knowledge in power systems, manufacturing automation, transportation system or as the case may be.

While courses do exist in various domain specific topics in various engineering departments, it is often from a design, control, and safety point of view, and not so much from the cyber security point of view. Cyber security should become a first-class design concern in the near future, and students in domain specific engineering disciplines must be trained in cyber security issues of their designs, especially in systems that use networked distributed control, SCADA systems, and sense-control-actuation paradigms of design.

While a number of courses do exist in cyber security – especially in network security – encryption, authentication, non-repudiation, and other protocols to establish veracity of identity, perimeter defense mechanisms through network security layers – a set of new courses are needed to upgrade the curriculum not only for outgoing computer engineers, but also to serve as courses for other disciplines where industrial automation, or infrastructure control systems are being taught.

The center's faculty in collaboration with faculty in other departments will design these courses, and possibly even offer some of the fundamental courses in the MOOC mode in order for engineering colleges outside IITK can also benefit from such courses.

Courses customized for government and industry executives in charge of cyber-security (such as executives of utilities, automotive industry, avionics etc) also will be designed and delivered as necessary by the center.

5.4.5 Outreach

Cyber-Security is yet to become a common topic of discourse among many utilities, and even among engineers who work at the critical infrastructure sector. The center has a responsibility towards the society at large, and one of the major goals of the center will be to create awareness. There are ways to create awareness – internships for students, short-term visits from industry to the center to collaborate and learn cyber-security challenge competitions among school and college students, creating webcasts and podcasts for general consumption, and even producing simple literature on do-s and do-nots for engineers, as well as consumers. We have a mission to create a cyber-security aware best practice guides which may be widely used by various utilities, and government sectors. We also want to provide course material, virtual lab setups to run experiments, and other teaching material for teachers in other colleges outside the IIT system to benefit all engineering colleges throughout India.

5.4.6 Consulting

Since one of our goals is to be *the hub* with expertise in cyber security in India, we will be engaged in consulting the government, industry, and utility sector in various capacities to upgrade their cyber security posture, and architectures. We also plan to consult on remediation of cyber threats found in various industry and government sector infrastructure, and also create some standard practices for these sectors to be up-to-date in their practices, technology procurement, and setups.

5.4.7 Postdoctoral and Doctoral Training

The TIH also plans to hire at least ten doctoral students every year – so as to have about fifty doctoral students in steady-state at the TIH (assuming 5 years graduation time) specializing in Cyber Security – in particular cyber security of critical infrastructure – which is essential for the man power not only in Indian academia but also in industry, startup and government agencies who will have the advanced skill and research acumen in Cyber security – which is missing currently in the Indian Eco system.

We also plan to hire at least four post-doctoral fellows each year – with a post-doctoral training period of 3 years each – having a steady state of twelve post-doctoral fellows at the TIH. This will create additional man power for industry and academia in India. Also, it is expected that some of the doctoral and post-doctoral students will be taking some of the technology they develop during their training and create startups within the TIH's start up ecosystem.

These PhDs and post-docs will be spread over IT Kanpur and three partnering institutions. In addition, hiring of PhD students and post-doctoral fellows will also be supported through R&D funding at other institutions.

5.4.8 Visiting Researchers and Faculty Fellows

The TIH will collaborate nationally with a number of institutes -- other than the partners IIT Kharagpur, IISc Bangalore, and IIIT Allahabad – and fund short term or medium-term visiting fellowships to broaden the network of researchers who would be working in the area of cyber security and in particular, the area of cyber physical system security.

Internationally, the TIH is already partnering with the Tandon School of Engineering at the New York University, and The Interdisciplinary Cyber Security Research Center at Tel Aviv University as IIT Kanpur's C3i lab already has a long-standing cooperation with these institutes. We plan to also invite researchers from these international collaborators as well as other internationally renowned centers and institutes for short term visits at the center so the cooperation can be enriched, and our engineers and students can gain further insight into the research at the international scale.

5.4.9 Cyber Security Policy, regulation and Law

At the TIH – the technology we develop, will be complemented by our interaction with the government bodies, regulators, and law makers in order to inform the various needs for new policy functions, regulatory requirements, and enhancement of IT act and other necessary legislative needs. Two of the project investigators in this TIH has served on various such committees including Cyber Security Committees of RBI, SEBI, CEA, UIDAI, CCTNS, and NATGRID. So, we believe that strong interaction among researchers and law makers/regulators/policy makers. With this in mind, we plan on fellowships in Cyber Law – in particular in the CPS domain – and work with them in enhancing their knowledge in threat models, the needs for regulatory plans, and formulation of better legislations. Two PIs in the project had once testified at the Parliamentary standing committee on Finance on Cyber Security of Financial systems and have found such interactions very useful for both sides.

5.4.10 Programs for Cyber Security Auditors

If Cyber Security of the country's critical infrastructure has to be enhanced, then strong audit principles, and auditing capabilities must be imparted to employees of audit companies. Just certification from CERT-In is not enough – as they need to be trained thoroughly. We plan to create programs to train the auditors – through C3i center, and also the SEAL Lab in IIT Kharagpur lab on Side Channel Analysis and Trojan detection. We believe such training programs of various durations can enhance the auditor's knowledge and provide tools and techniques in their arsenal to provide proper audit and advise to the various industrial sectors, utilities and government agencies.

5.4.11 International Outreach

Since 2018, IIT Kanpur's C3i Lab has been running two courses of two-weeks duration each under the International Technology and Economic Cooperation (ITEC) program. We have trained IT professionals from various countries in Africa such as Kenya, Ghana, Tanzania, Nigeria, Senegal, Sudan, south-east Asian countries such as Malaysia, Philippines, and South Asian counties such as Bhutan, Bangladesh, and even some south American countries. This year also we are repeating the same. The first training program "Introduction to Cyber Security for IT professionals" and second "Intermediate Cyber Security for IT Professionals" have been quite well received by over 50 international IT professionals last year, and this

year's program is running at the moment. Under the TIH with more man power and more knowledge and laboratory facilities – we should be able to extend these programs further.

5.4.12 Summary

Overall, given our experience in manpower and skill development in cyber security – and cyber security of CPS – we are well poised to create a vibrant manpower & skill development activity within the proposed TIH. This would include curriculum development, online and offline courses, executive training programs, programs customized for specific sectors in Critical infrastructure, international programs. We also plan to create researchers and scientists with focused skill in CPS cyber security through our degree programs, post-doctoral fellowships, visiting fellowships.

6 Strategy

This section analyses alternative strategies to the one proposed by us to secure digital and cyber physical systems, and highlights their drawbacks compared to ours.

6.1 Alternative Strategy: Buy Technology

This is not feasible. Much of the advanced technology related to cyber security is not exported by the countries that develop them. And the technology that does get exported, comes at a prohibitive cost. In addition, there is always the possibility with imported technology that it can be stopped from working during a conflict situation through hidden trojans.

6.2 Alternative Strategy: Funding Through SERB/DST

Funding the R&D and technology translation through SERB/DST has been going on for a while. Given the broad focus of these agencies, attention to cyber security gets diluted. Therefore, the present model is being attempted where the hub will act as a source for funding and promotion of cyber security related activities in the country.

7 Target Beneficiaries

C3ihub at IIT Kanpur will engage dedicated Indian start-ups and other TIH partners and will only be focused on research and development of various tools, technique and best practices for national security. Ecosystem covers the following key areas.

1. Securing government systems: Protection of government assets, infrastructure and systems from cyber threats is paramount for the upkeep of our socio-economic health and military might. It is vital for safety, security, growth and sustenance of the nation's economy, protection of its citizens, wealth, and infrastructure.

2. Securing business cyber ecosystem: A healthy and resilient cyber ecosystem is required for the enterprises to effectively contribute to the progress of the nation. For this to succeed, all the stakeholders need to collaborate to cohesively contribute to security

3. Creating cyber secure society: A society driven by cyber safe culture is less susceptible to cyber adversaries. Creating awareness and training people on cyber security are required to attain a true cyber secure society.

4. Building technological and human capacity: Creation of indigenous tools & human capacity and capability is imperative to not only protect Indian cyber space but also to make India globally competitive in cyber security.

7.1 Key Beneficiaries

1. Critical Infrastructure
    a. Power & Energy
    b. Transport
    c. Gas
    d. Industrial
    e. Telecommunications
2. Banking, Financial & Insurance
    a. Public sector banks
    b. Private sector banks
    c. NBFCs
    d. Stock Exchange
    e. Insurance Companies
3. Government
    a. Indian Armed Forces
        i. Indian Airforce
        ii. Indian Army
        iii. Indian Navy
    b. Agencies under MHA
    c. DRDO
    d. ISRO
    e. Agencies under PMO
4. Strategic and Business Enterprises

8 Legal Framework

The Program will be managed by a separate legal entity in the form a "**Not For Profit**" Company (limited by guarantee, not having share capital) which shall be registered under Section 8 of the Companies Act 2013. This Section 8 Company (the "**Company**") shall have 100% ownership of IIT Kanpur and shall take care of all strategic and operational tasks of the TIH.

The Section-8 Company shall be operated and managed by its separate Board of Directors. These members will be responsible to oversee the activities of the Company and will be accountable for its overall performance. The Books of accounts of the Company will be audited by the independent statutory auditors. The Auditor has to give his view independently without being influenced in any manner. He will check the financial records and will give his opinion thereon in the audit report. It helps the stakeholders to rely on financial statements.

9 Environmental Impact

The activities under the hub will not have any *significant additional* impact on the environment. All the verticals already use equipment which have varying impact on the environment. The cyber security part, being purely based on software, will not adversely impact the environment except for consuming additional electricity and generating some amount of heat due to use of computing power.

10 Technology

All the activities of the hub require use of computers, which is standard technology.

11 Management Plan

It is proposed that a separate Section 8 company be established to take care of all strategic and operational tasks of the TIH.

Board of Directors

The Section-8 Company shall be governed by its Board of Directors (BOD). This will consist of:

- Director, IIT Kanpur as Chairman
- Deputy Director, IIT Kanpur
- Dean R&D, IIT Kanpur
- Program Director

The BOD shall collectively direct the company's affairs while meeting the appropriate interests of its internal and external stakeholders. The BOD shall be responsible for creating suitable strategies and plans for the attainment of objects of the Company. The Board will approve appropriate policies of the Company such as HR Policy, Purchase Policy, Travel Policies etc. and other relevant rules & regulations of the Company.

Apart from the Board, the hub shall have a Hub Governing Body (HGB) consisting of:

- Director, IIT Kanpur as chairman
- Program Directors
- Members associated with IIT Kanpur working in the TIH domain
- External members from industry, investment world and government agencies

The Hub Governing Body shall provide all the feasible mentoring and advisory support to the BOD for enabling the Company to achieve its milestones.

The operations of the Hub will be handled by a Management Team consisting of:

- Program Directors
- Chief Executive Officer
- Chief Operating Officer
- Chief Finance Officer
- Managers for each stream
- Financial and legal support team
- Marketing and outreach team
- Support staff

Project Director(s)

Faculty member(s) shall be designated as Project Director(s) who shall be heading the Mission.

Chief Executive Officer (CEO)

The Company shall also have its Chief Executive Officer who shall report to the Project Director(s) and shall oversee all the operations of the Company.

Chief Operating Officer (COO)

Day-to-day operations will be supervised by a Chief Operating Officer who will be assisted by managers, financial, legal, marketing, and outreach staff.

Chief Financial Officer (CFO)

The Chief Financial Officer shall be responsible for the financial management of the Company. He will ensure proper financial standards and safeguards to be followed by the Company.

12 Finance

12.1 Budget Details

Overall budget for five years is Rs 170 Crores. Yearwise breakup in recurring and non-recurring categories is as follows:

Budget Head / Year	Year-1	Year-2	Year-3	Year-4	Year-5	Total
Recurring	19.82	28.86	30.00	28.42	33.46	**140.56**
Non-recurring	26.87	1.17	0.93	0.35	0.12	**29.44**
Total in Rs Crores	**46.69**	**30.03**	**30.94**	**28.77**	**33.57**	**170.00**

For the first-year budget, Rs 7.25 Crores is already received of which Rs 5.25 Crores is for recurring and Rs 2 Crores is for non-recurring components. Hence, Rs 14.57 Crores towards recurring, and Rs 24.87 Crores towards non-recurring is outstanding (a total of Rs 39.44 Crores).

The year-wise breakup of the budget in major categories is given in the tables below. All the numbers below are in Rs Lakhs.

Budget Head	Year-1	Year-2	Year-3	Year-4	Year-5	Total
Manpower (Managerial)	131.00	131.00	137.55	137.55	144.10	**681.20**
R&D @IIT Kanpur	1533.22	326.50	389.38	415.63	454.55	**3119.27**
R&D @Other Institutions	1904.17	827.33	764.67	494.00	407.13	**4397.30**
HRD and Skill Development	147.25	195.25	250.06	278.06	279.88	**1150.50**
Travel @IIT Kanpur	30.00	30.00	30.00	30.00	30.00	**150.00**
Innovation, Entrepreneurship and Startup Ecosystem	400.00	1050.00	1050.00	1050.00	1550.00	**5100.00**
International Collaboration	30.00	50.00	60.00	60.00	60.00	**260.00**
Capex Items	100.73	0.00	0.00	0.00	0.00	**100.73**
Consumables/Contingency	68.50	68.50	71.93	71.93	75.35	**356.20**
Rentals & service charges	324.00	324.00	340.20	340.20	356.40	**1684.80**
Total	**4668.86**	**3002.58**	**3093.78**	**2877.36**	**3357.41**	**17000.00**

A more detailed breakup, expanding on the R&D expenditure is in the table below.

Budget Head	Year-1	Year-2	Year-3	Year-4	Year-5	Total
Manpower (Managerial)	131.00	131.00	137.55	137.55	144.10	**681.20**
Manpower (Technical)	477.50	570.50	687.38	734.63	803.35	**3273.35**
Technology Development (institutions other than IITK and partners)	466.67	583.33	466.67	175.00	58.33	**1750.00**
Equipment (IIT Kanpur)	1255.72	0.00	0.00	0.00	0.00	**1255.72**
Equipment (IITKGP+IISc+IIITA)	1237.50	0.00	0.00	0.00	0.00	**1237.50**
HRD and Skill Development	147.25	195.25	250.06	278.06	279.88	**1150.50**
Travel @IIT Kanpur	30.00	30.00	30.00	30.00	30.00	**150.00**
Innovation, Entrepreneurship and Startup Ecosystem	400.00	1050.00	1050.00	1050.00	1550.00	**5100.00**
International Collaboration	30.00	50.00	60.00	60.00	60.00	**260.00**
Capex Items	100.73	0.00	0.00	0.00	0.00	**100.73**
Consumables/Contingency	68.50	68.50	71.93	71.93	75.35	**356.20**
Rentals & service charges	324.00	324.00	340.20	340.20	356.40	**1684.80**
Total	**4668.86**	**3002.58**	**3093.78**	**2877.36**	**3357.41**	**17000.00**

We now give detailed justification of above budget, categorized by institutions.

12.1.1 IIT Kanpur

Expenditure at IIT Kanpur is captured in the following table.

Budget Head	Year-1	Year-2	Year-3	Year-4	Year-5	Total
Manpower (Managerial)	131.00	131.00	137.55	137.55	144.10	**681.20**
Manpower (Technical)	277.50	326.50	389.38	415.63	454.55	**1863.55**
Travel	30.00	30.00	30.00	30.00	30.00	**150.00**
HRD and Skill Development	147.25	195.25	250.06	278.06	279.88	**1150.50**
Innovation, Entrepreneurship and Startup Ecosystem	400.00	1050.00	1050.00	1050.00	1550.00	**5100.00**
International Collaboration	30.00	50.00	60.00	60.00	60.00	**260.00**
Equipment	1255.72	0.00	0.00	0.00	0.00	**1255.72**
Capex Items	100.73	0.00	0.00	0.00	0.00	**100.73**
Consumable/Contingency	33.50	33.50	35.18	35.18	36.85	**174.20**
Rentals & service charges	324.00	324.00	340.20	340.20	356.40	**1684.80**
Total	**2729.70**	**2140.25**	**2292.36**	**2346.61**	**2911.78**	**12420.70**

12.1.1.1 Managerial Manpower

It is proposed to hire a CEO, COO, lawyers, auditors, and other managers to run the hub. Lawyers and auditors will be on sharing basis with the Incubation Center at IIT Kanpur. The breakup of their expenditure is:

Designation	No of person/s	Year-1	Year-2	Year-3	Year-4	Year-5	Total
CEO	1	24.00	24.00	25.20	25.20	26.40	**124.80**
COO	1	18.00	18.00	18.90	18.90	19.80	**93.60**
IP, Patent and Contract Lawyer	1	6.00	6.00	6.30	6.30	6.60	**31.20**
Marketing and Outreach Personnel	1	6.00	6.00	6.30	6.30	6.60	**31.20**
Project Management and Industry Liaison Managers	4	72.00	72.00	75.60	75.60	79.20	**374.40**
Part-Time Accounts Auditor	1	5.00	5.00	5.25	5.25	5.50	**26.00**
TOTAL (Managerial)		**131.00**	**131.00**	**137.55**	**137.55**	**144.10**	**681.20**

In the salaries above, and in subsequent calculations, we have incorporated a 5% increase after two and four years.

12.1.1.2 Technical Manpower

Technical manpower will form the backbone of R&D work. This includes masters, PhD, postdocs, and research engineers.

Designation	No of person/s	Year-1	Year-2	Year-3	Year-4	Year-5	Total
UG Fellowships	40	12.00	12.00	12.6	12.6	13.2	**62.40**
M. Tech/MS Fellowships	10	24.00	24.00	25.20	25.20	26.40	**124.80**
PhD Fellowships	5	25.00	50.00	76.25	102.50	130.00	**383.75**
Post-Doctoral Fellowships	2	24.00	48.00	73.20	73.20	73.20	**291.60**
Research Engineers (Senior RE, Junior RE, Associate RE, Project Executive RE)	25	180.00	180.00	189.00	189.00	198.00	**936.00**
Support Staff (Technical and Non-Technical)	5	12.50	12.50	13.13	13.13	13.75	**65.00**
TOTAL (Technical)		**277.50**	**326.50**	**389.38**	**415.63**	**454.55**	**1863.55**
TOTAL		**408.50**	**457.50**	**526.93**	**553.18**	**598.65**	**2544.75**

12.1.1.3 Travel

At present, there are ten industry partners and three national institute collaborators. These numbers will increase significantly within a year. There will be multiple visits, particularly of students and researchers, between IIT Kanpur and its partners. Also, there will be meetings with SERB and government entities such as NCSC, CEA, DSCI, and various conferences within the country. We estimate about 200 persons domestic

travels between collaborating partners, industry partners, students and engineers of the TIH to the collaborating partners, and various meetings per year. Each person domestic travel costs about 25,000 INR on average depending on the length of stay, the hotel cost etc. So we are estimating about 50 Lacs in domestic travel cost for the TIH employees and faculty.

12.1.1.4 HRD and Skill Development

For training purposes, following is planned:

- Ten MOOC courses, each costing Rs 5 lakhs
- Four workshops every year for faculty development, employee and student training, each costing Rs 5 lakhs
- Twenty five summer interns to be hosted at the Hub every year, each costing Rs 25K
- Outreach program for creating awareness in the society, costing Rs 10 lakhs per year

It is proposed to establish ten chair positions for senior faculty and twenty fellowships for junior faculty working in cyber security all over the country. These will be used to attract faculty in cyber security as well as recognize faculty achievements in the domain. Each chair will carry a stipend of Rs 1 lakh per month and fellowship Rs 50K per month.

Intiative	No per year	Year-1	Year-2	Year-3	Year-4	Year-5	TOTAL
MOOC Courses		15.00	15.00	20.00			**50.00**
Workshops	4	20.00	20.00	21.00	21.00	22.00	**104.00**
Summer Internships	25	6.25	6.25	6.56	6.56	6.88	**32.50**
Outreach	1	10.00	10.00	10.50	10.50	11.00	**52.00**
Chair Professors		48.00	72.00	96.00	120.00	120.00	**456.00**
Fellowships		48.00	72.00	96.00	120.00	120.00	**456.00**
TOTAL		**147.25**	**195.25**	**250.06**	**278.06**	**279.88**	**1150.50**

12.1.1.5 Innovation, Entrepreneurship and Startup Ecosystem

It is envisaged that twenty five startups will be initiated every year across the country nucleated by TIH. Each one of these, after due evaluations, will be provided a seed grant of Rs 10 lakhs and salary for two founders at Rs 50K per month for two years, resulting in an investment of Rs 22 lakhs in each startup.

After two years, it is expected that 20% of these startups will be successful. At that time, an additional investment of up to Rs 100 lakhs will be made in each of these to help them scale up.

12.1.1.6 International Collaboration

With four international collaborating institutes, a number that is likely to increase, we plan to have student and faculty exchanges for short durations. This support will also be provided to partner institutions in the country (and is not included in their budget). We are budgeting for 15 visits per year with an estimate of Rs 4 lakhs per visit (travel, stay, and other expenses).

12.1.1.7 Equipment

Following is the detailed list of equipment planned to be purchased at IIT Kanpur with estimated costs. Their justification is provided in Sections 2 and 3.

Generic Name, Model No, (Make)/ Justification	Quantity	Unit Cost	Estimated Cost
Smart Board: H82DMERTBC/XL (Samsung)	1	8.00	**8.00**
Network Tap: GigaVUE-HC2 (Gigamon)	6	0.60	**3.60**
Desktops: ThinkCenter i-7 Core (Lenovo)	15	0.60	**9.00**
Laptop: Ideapad S 540 (Lenovo)	10	0.70	**7.00**
Workstation: Precision 7820 (Dell)	3	6.00	**18.00**
Mac Laptop: Macbook Pro (Apple)	2	2.00	**4.00**
Printer: LaserJet MFP M436nda (HP)	10	1.00	**10.00**
Amazon Cloud Services (AWS): AWS instances subscription	1	6.00	**6.00**
High End Desktop Intel SGX Skylake desktop, equipped with two NVdia Pascal GPUs. 32GB RAM and 1TB storage (Intel)	2	7.00	**14.00**
Rack Servers with 10 cores Power Edge with minimum 4 intel xeon gold 5115 2.4G, 10C / 20T, 10.4GT/s, 14 M cache, Turbo, HT (Dell)	8	14.60	**116.80**
Firewall CUSCO ASA5508 (CISCO)	6	1.00	**6.00**
KVM Switch ATEN 17" 16-port LCD KVM. Daisychainable. Multi- platform. 2nd Console USB device port.LED illuminati (ATEN)	2	1.20	**2.40**
Cyber Range for Research, Education, and Training For red-team/blue-team cyber exercise capabilities for research in developing educational lessons, human skill development, training programs – a cyber range is an essential setup.	1	400.00	**400.00**
Basic communication equipment including antennas AD-FMCOMMS5-EBZ – UAV communications evaluation hardware	1	1.00	**1.00**

Simpulse SL-200 module	1	12.00	**12.00**
Tracking/alignment setup including INS, gimbal			
Mobile tracker antenna setup with tilting mast, variable height	1	1.15	**1.15**
INS	1	17.25	**17.25**
Gimbal	1	1.15	**1.15**
Long range communication setup including Satcom (Cobham)			
Satcom transceivers, antennas, service license	1	57.50	**57.50**
Workstations for primary ground station, back up/monitoring stations			
Getac Ground computer B300	1	1.84	**1.84**
Getac Remote console F110	1	4	**4.00**
Aircraft addressing and tracking systems (ADS-B)			
ADS-B (Garmin) 1 unit	1	1.725	**1.73**
Signal Intelligence			
Avantix Flashhawk (COMINT/SIGINT/ELINT)	1	23	**23.00**
Radar	1		
Fortem Trueview R20 Radar	1	15	**15.00**
NPNT authentication server			
NPNT SSL certificate authentication server	1	5.75	**5.75**
Test Facility/Hardware			
Aerospace HIL Testbench – Opal RT	1	57.5	**57.50**
Oscilloscope Teledyne LeCroy HDO4104A	1	16.75	**16.75**
Logic anlayzer (16 Channel, USB based)	1	1	**1.00**
Tektronix RSA 507A [9 Khz to 7.5 Ghz], Handheld with display on device.	1	13.8	**13.80**
Tektronix TTR506A USB vector network analyzer [100 KHz to 6 GHz	1	13.8	**13.80**
Keysight N5182B signal generator	1	34.5	**34.50**
Antenna modelling software Ansys HFSS	1	5.75	**5.75**
Programmable power supply Bench top – TDK Lambda ZUP6-66	1	1.15	**1.15**
Power supply surge generator(voltage/current) – Test facility	1	34.5	**34.50**
RF synthesizer (Radiated RF immunity testing), Power amplifiers – Test facility	1	1.15	**1.15**
Conducted RF immunity testing	1	57.5	**57.50**
ESD generator	1	28.75	**28.75**
AFJ FFT 3030 EMI test receiver	1	1.15	**1.15**
Crystek RF lab kit	1	0.75	**0.75**
LIDAR (landing precision, fail safe landing)	1	97.75	**97.75**

Epsilon Gimbal System (MWIR, EO, LRF and Illuminator)	1	46	**46.00**
Octopus UAV IP Data Link	1	11.5	**11.50**
Testing Aircraft and Equipment's	1	28.75	**28.75**
Rate Table	1	57.5	**57.50**
TOTAL @IITK			**1255.72**

12.1.1.8 Capex Items

Some racks are required for housing servers costing approximately Rs 2 lakhs. Institute will be allocating 30,000 sqft of space for the TIH and furnishing the space would cost approximately Rs 1 Crore.

12.1.1.9 Rental

The space allocated by the institute will be given on rent to the TIH. Institute, as per its Board approved policy, charges Rs 90 per square ft per month as rent which includes electricity, air-conditioning, water, and maintenance. This translates to Rs 3.24 Crores per year. As for salaries, escalation of 5% has been included after two and four years.

12.1.2 IIT Kharagpur

IIT Kharagpur will focus on automotive and hardware security closely working with the TIH. The budget breakup for IIT Kharagpur is given below. They will have four MTech and two PhD students per year, apart from one postdoc and ten research engineers.

Budget Head	**Nos**	**Year-1**	**Year-2**	**Year-3**	**Year-4**	**Year-5**	**Total**
UG Fellowships	20	6.00	6.00	6.30	6.30	6.60	**31.20**
M. Tech/MS Fellowships	4	9.60	9.60	10.08	10.08	10.56	**49.92**
PhD Fellowships	2	10.00	20.00	30.50	41.00	52.00	**153.50**
Post-Doctoral Fellowships	1	12.00	24.00	36.60	36.60	36.60	**145.80**
Research Engineers (Senior RE, Junior RE, Associate RE, Project Executive RE)	10	72.00	72.00	75.60	75.60	79.20	**374.40**
Total Manpower		**109.60**	**131.60**	**159.08**	**169.58**	**184.96**	**754.82**
Equipment		1185	0	0	0	0	**1185**
Consumables/Contingency		20	20	21	21	22	**104**
Total		**1314.60**	**151.60**	**180.08**	**190.58**	**206.96**	**2043.82**

The details of the equipment for creating automotive security testbed and hardware testing lab are:

Generic Name, Model No. , (Make)/ Justification	Quantity	Unit Cost	Estimated Cost
Automotive security Testbed For Automotive security research, benchmarking and training	1	85.00	**85.00**
Side Channel and Trojan Detection and Testing Lab Building Side-Channel Analysis and Trojan and Counterfeit Detection Lab setup	1	1100.00	**1100.00**
TOTAL @IITKGP			**1185.00**

12.1.3 IISc Bangalore

IISc Bangalore will work on multi-party and trusted computation aspects. Their budget breakup is:

Budget Head	Nos	Year-1	Year-2	Year-3	Year-4	Year-5	Total
M. Tech/MS Fellowships	4	9.60	9.60	10.08	10.08	10.56	**49.92**
PhD Fellowships	1	5.00	10.00	15.25	20.50	26.00	**76.75**
Post-Doctoral Fellowships	1	12.00	24.00	36.60	36.60	36.60	**145.80**
Research Engineers (Senior RE, Junior RE, Associate RE, Project Executive RE)	4	28.80	28.80	30.24	30.24	31.68	**149.76**
Total Manpower		55.40	72.40	92.17	97.42	104.84	**422.23**
Equipment		45	0	0	0	0	**45**
Consumables/Contingency		10	10	10.5	10.5	11	**52**
Total		**110.40**	**82.40**	**102.67**	**107.92**	**115.84**	**519.23**

They will have four MTech and one PhD students along with one postdoc and four research engineers. They will setup a full memory encryption lab as per following details:

Generic Name ,Model No. , (Make)/ Justification	Quantity	Unit Cost	Estimated Cost
Full Memory Encryption Lab Two high end Intel servers, one equipped with Skylake (server edition) motherboard for doing Intel MPK research, and another equipped with AMD Ryzen- enabled motherboard for doing research on full- memory encryption technology of AMD. Both servers equipped with 4 Nvidia Turing GPUs for running machine learning workloads, which are now routinely used as evaluation workloads in systems papers. 64GB RAM and 1TB storage in each server	1	45.00	45.00
TOTAL @IISc			**45.00**

12.1.4 IIITA Prayagraj

IIITA Prayagraj will setup an IoT security lab to investigate possible weaknesses in low power settings. Their budget breakup is:

Budget Head	Nos	Year-1	Year-2	Year-3	Year-4	Year-5	Total
UG Fellowships	20	6.00	6.00	6.30	6.30	6.60	**31.20**
M. Tech/MS Fellowships	4	9.60	9.60	10.08	10.08	10.56	**49.92**
PhD Fellowships	1	5.00	10.00	15.25	20.50	26.00	**76.75**
Post-Doctoral Fellowships	0	0.00	0.00	0.00	0.00	0.00	**0.00**
Research Engineers (Senior RE, Junior RE, Associate RE, Project Executive RE)	2	14.40	14.40	15.12	15.12	15.84	**74.88**
Total Manpower		**35.00**	**40.00**	**46.75**	**52.00**	**59.00**	**232.75**
Equipment		7.5	0	0	0	0	**7.5**
Consumables/Contingency		5	5	5.25	5.25	5.5	**26**
Total		**47.50**	**45.00**	**52.00**	**57.25**	**64.50**	**266.25**

They will employ four MTechs, one PhD student per year, and two research engineers. The IoT lab would cost Rs 7.5 lakhs.

12.1.5 Open Calls

The Hub will run calls for funding R&D work in the first three years. Project funding will be of two kind: full project (average support of Rs 30 lakhs) and small project (average support of Rs 10 lakhs). In each of the first two years, fourteen full projects and twenty-eight small projects are expected to be approved and in the third year, seven full projects and fourteen small projects. Total funding support is Rs 17.5 Crores.

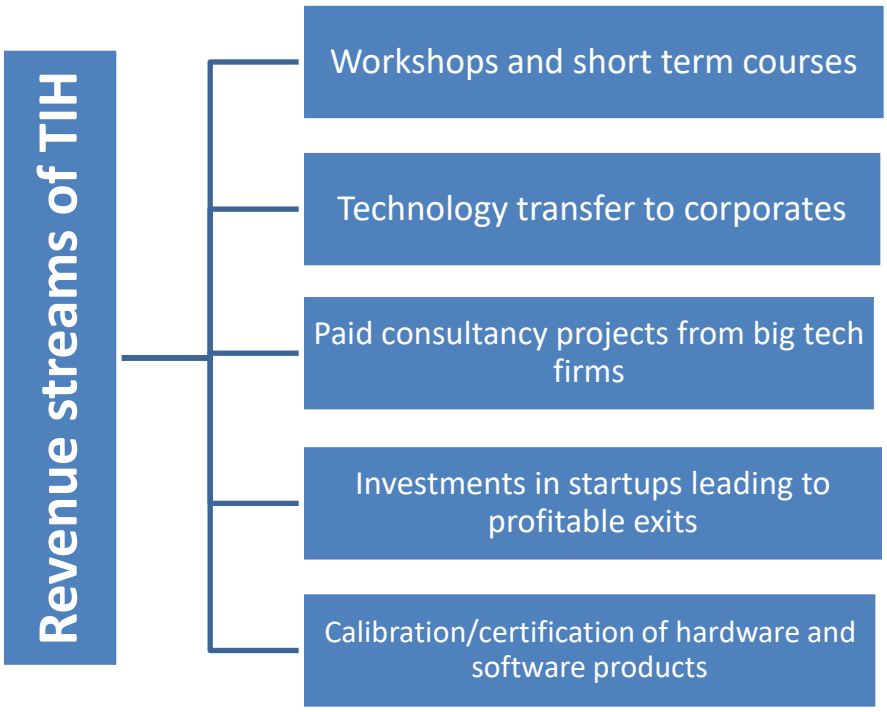
12.2 Plan for revenue generation and sustainability

The C3i center at IIT Kanpur already has a responsive system and has been working with multiple industry and government partner. We have been working on technology transfer, joint development with multiple industries, vulnerability disclosures, and advisories to the industry. Further, a team will be recruited and trained on market research, interacting with Data Security Council of India (DSCI) – A Nasscom organization with whom IIT Kanpur recently inked a Memorandum of agreement.

Also, the proposed TIH plans to create a malware repository, a repository for cyber security experimental data collected from our test-beds, and other data sources. These will help us analyse the threat landscape in India, and accordingly tailor our models, and tailor advisories in coordination with DSCI.

In terms of sustainability – we have a concrete plan. Since the inception of the TIH, the first four year expenses will be covered fully by the budget from SERB. The final year budget will be 70% from SERB, and 30% from other avenues through industry engagements, and then onwards, the TIH must go into self-sustenance mode. We propose the following steps towards revenue generation and self-sustainability.

- Engage in extensive research, knowledge generation and product development of the technologies discussed above.
- License out the technologies to selected entrepreneurs whose startups shall work on commercialization of the product, upscaling and business development.
- The startup will be supported by the TIH for a period of two years through fellowships to individuals as well as seed funding support necessary for business development, followed by a higher grant to promising ones. The startup support plan is discussed in detail in the Entrepreneurship section of this proposal.
- Once the startup shall start generating revenues and it shall repay the TIH through royalty fees. TIH shall also hold equity in these startups and shall seek exits when any of these startup companies receive series funding from VCs.
- In the 3rd year of operation, the TIH shall hire a marketing team for aggressive promotion of its activities and research initiatives for bringing consultancy projects from big tech companies in India and abroad. The TIH marketing team shall also promote technology transfer of developed/under-development products to corporate entities for direct licensing.
- Calibration of hardware products by developing a comprehensive in-house expertise wherein industry can get their hardware/software products calibrated by the TIH which may also act as a validation of the product.
- Paid skill training programs and short-term courses on various aspects of cybersecurity by in-house and invited experts by conducting regular technology and innovation workshops.



We now provide the breakup of expenditure and revenue.

12.2.1 Expenditure

Major capital expenditure for the TIH in terms of equipment, and test-bed etc, will be in the first year. Thereafter, most of the expenditure is to be in paying salary to engineers and employees, student and post-doctoral stipends, travel, contingency, consumable and workshops. Numbers for personnel will be similar to 5th year of TIH with some exceptions:

Designation	**No of person/s**	**Yearly Expenditure**
CEO	1	26.40
COO	1	19.80
IP, Patent and Contract Lawyer	1	6.60
Marketing and Outreach Personnel	1	6.60
Project Management and Industry Liaison Managers	5	99.00
Part-Time Accounts Auditor	1	5.50
TOTAL (Managerial)		**163.90**
M. Tech/MS Student Fellows	10	26.40
PhD fellows	5	130.00
Post-Doctoral Fellows	3	109.80
Research Engineers (Various Levels – Senior RE, Junior RE, Associate RE, Project Executive RE)	25	198.00
Support Staff (Technical and Non-Technical)	5	13.75
TOTAL (Technical)		**477.95**
Travel		150.00
Workshops	4	22.00
Startup grants		1550.00
Contingency		50.00
Rental		356.40
TOTAL		**2770.25**

Some observations about the budget above:

1. Because of collaboration, especially foreign collaboration, the travel budget per year is kept at Rs 150 lakhs per year.
2. For contingency and consumables, we have budgeted Rs 50 Lakhs (maintenance and upgrade of test-beds, replacing faulty components, digital certification renewal, domain name renewal, replacing old desktops etc)
3. The TIH will continue to support startups in the same way.

The total annual expenditure is approximately Rs 28 Crores, which is about Rs 7 Crores less than fifth year due to stopping of funding to other institutions.

12.2.2 Revenue

The projected revenue is:

Activity	Revenue
Executive Training Program	200
Industry support	200
Testing services	300
Project funding	200
Earnings from startups	3000
TOTAL	**3900**

The above calculation has the following basis:

1. Industrial and Executive training program revenue will be approximately Rs 2 Crores (Already C3i started an executive program with an intake of 50 participants – who will be trained over 6-month period via TalentSprint platform and the revenue projection for 2020 is Rs 1 Crore for C3i itself).
2. Revenue from Industrial funds (as the technology development takes off, we assume that industries will either want to have customize research agreements for specific technology, or technology license technology or even produce revenue by marketing our technology products) is projected to be Rs 2 Crores.
3. We plan to provide testing services at the various test labs created under the TIH, audit service (C3i has unofficially done audits for multiple facilities already) and we also plan on providing consultancy and other cyber security planning, framework implementation advice etc. We expect this to generate a revenue of Rs 3 Crores.
4. We will continue to write proposals against various government programs at the MEITY, SERB, DST and other organizations and hope that we can generate another Rs 2 Crore from the various research funding sources.
5. In lieu of funding promising startups with grants of Rs 120+ Lakhs, the TIH will acquire about 10% equity of the company (the exact breakup to be decided by the Board of TIH). On average, five such startups are planned to be funded every year. Once they become successful, their combined worth will very likely exceed Rs 300 Crores. Hence, this will earn the TIH Rs 30 Crores per year.

Therefore, our projected revenue from year six onwards is about Rs 39 Crores, well in excess of projected expenditure.

13 Time Frame

In this section, we describe the major activities and products grouped into distinct categories followed by a number of milestones to archive and finally a time line for these milestones. We first categorize the facilities and activities into groups.

Test-beds

- Cyber Range (Red-Team/Blue-Team Exercise Testbed)
- Automotive Platform Test-bed
- IoT Security Test Bed

Test-facility

- Industrial Automation Component hardware/software in-the-loop Test Facility
- Side Channel and Trojan Detection Test lab
- IoT device test facility

Methodology Development Activities

- Secure Boot
- Multi-party Computation based Secret Sharing
- Fuzz Testing of O/S and Applications
- Memory Hierarchy Security
- Novel Side Channel Analysis
- Protocol Reverse Engineering and Vulnerability Discovery
- Firmware and Application Level Vulnerability Assessment and Penetration Testing
- IEC 62443 implementation methodology
- NIST Cyber Security Framework Implementation Methodology
- Cyber Asset management Methodology
- National UAV Security Standard
- National Automotive Security Standard
- IoT Security Standard

Data Repositories

- Malware Database
- Threat Model Database
- Dataset for Intrusion Detection of CPS behavior

Tools

- Fuzz Testing Tools
- CPS honeypots
- Malware Analysis Tools
- Threat Intelligence Tools
- VAPT Tools for CI-CPS

- VAPT tools for Automotive CPS
- VAPT Tools for UAV CPS
- Cyber Asset management tool
- Application specific firewall
- Intrusion Detection tool for CI-CPS
- Intrusion Detection in Automotive
- Intrusion Detection in UAVs
- Side Channel Analysis Tools
- Trojan Detection Test Tools

Startup activities

The current plan is to have call for proposals for start up open to anyone who is interested to open a start up in the cyber security domain. This includes students, faculty, engineers, post-doctoral fellows, and visiting fellows to the TIH. Based on the proposals, and prototypes developed, every year up to 5 new startups will be funded for 2 years each. After 2 years they have to graduate from our incubation facility to independent organizations. If successful and the start up can afford, they can be given space in IIT Kanpur Technopark as well. So the goal is to spawn 25 startups over 5 years.

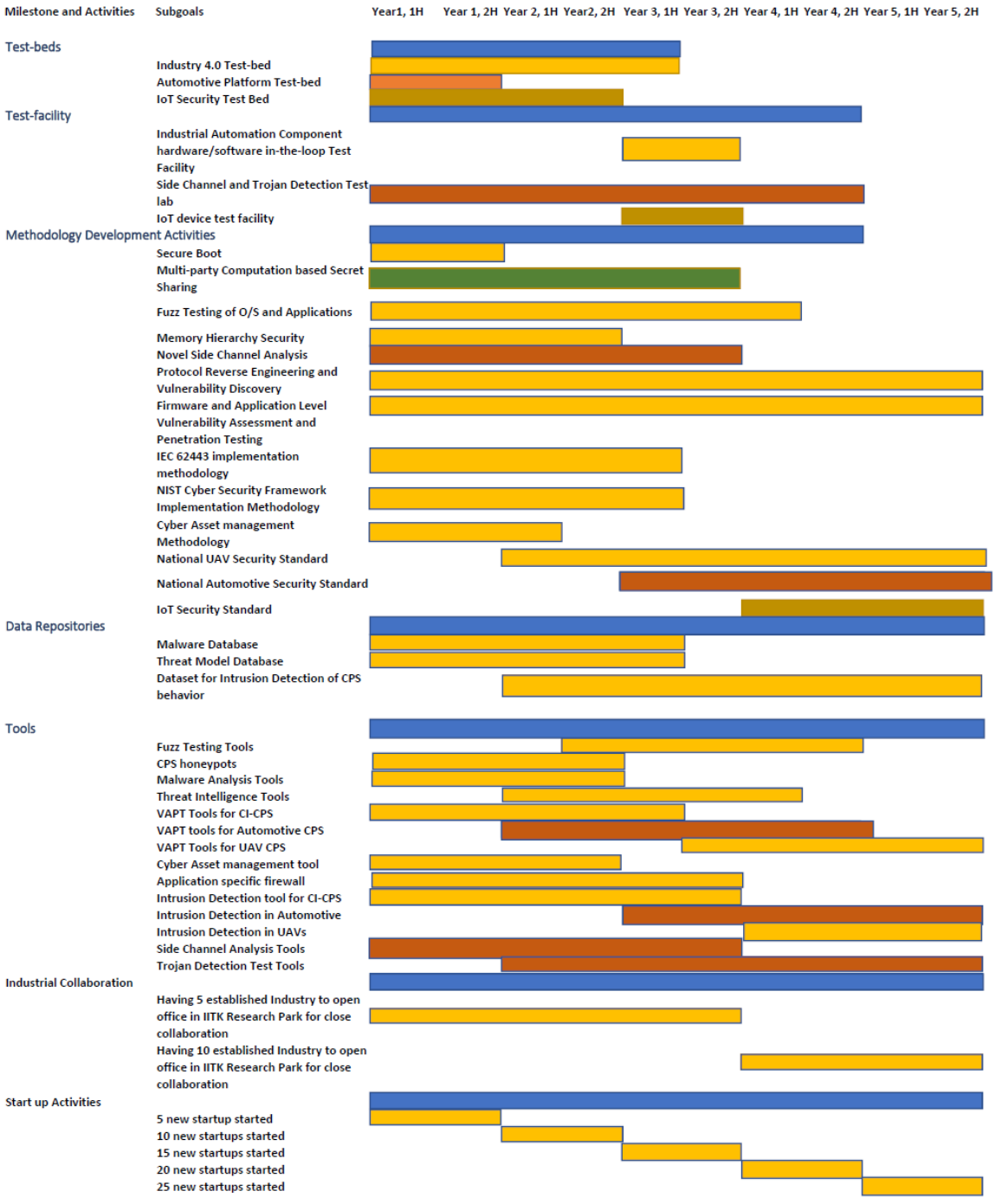
Industrial Interaction activities

IITK Technopark provides facilities and space for established companies to open satellite offices on campus so that they can work more closely with the research groups, make use of the facilities including test-beds, and labs. Our goal is to attract at least 10 established companies (including those who graduate from startup incubation program of the TIH) in cyber security domain to the technopark.

13.1 Major Milestones

- First round of project sanctions to other institutions
- Second round of project sanctions to other institutions
- Opening C3i Existing Test-beds for Industrial Partner
- Automotive Security Test-bed Completion
- IoT Security Test-bed completion and Lab Completion
- Side Channel Analysis and Trojan Detection Lab completion
- Completion of Methodology Development Activities
- Completion of Tools planned
- Total 25 start ups establishment
- 10 industries open offices in Technopark

13.2 GANTT Chart



14 Cost Benefit Analysis

As per a 2019 study (https://www.pwc.in/assets/pdfs/consulting/cyber-security/cyber-security-india-market.pdf) of the Indian Cyber Security Market segment, jointly done by PwC along with DSCI, the cyber security market in India is expected to grow from USD 1.97 billion in 2019 to USD 3.05 billion by 2022 at a CAGR of 15.6%—almost one and half times the global rate. Among these, in 2019, the cyber security services sector accounted for 47.92%, and Cyber Security Product market for 52.07% (USD 1030 million) in 2019. The projection for 2022 is that the product market will grow to USD 1643 million which will account for 53.81% of the cyber security market as a whole. If we project growth at the same rate of 15.6% yearly, the market size for products will become USD 2.538 billion USD in 2025. Since most of the products are from abroad, if indigenous cyber security products developed at TIH capture even 20% of this market in India by 2025, it amounts to an earning of USD 508 million, or equivalently, Rs 3840 Crores. The proposed investment in the TIH is Rs 170 crores, so this amounts to around 22x ROI.

The above calculation is only for business value – the strategic benefits of securing critical infrastructures and information are not measurable in monetary terms.

15 Risk Analysis

The main risk is due to lack of cyber security researchers in the country. Although the hub plans to help recruit many, if it does not happen then the activities of the hub will get impacted. In addition to this, we list below the risks associated with major technology developments that we have proposed.

Technology to be developed	Risks
Industrial Scale Test-Beds for Cyber Security Experimentation: **CI-CPS Test-Bed (IITK)** **IoT Test-Bed in IIITA** **Automotive Security Test-bed at IITKGP** **UAV Test-bed in IITK**	Delays due to tendering issues could cause delays in procuring components for test-bed, Hiring Engineers to operate test-bed are expensive
Side Channel and Trojan Testing Lab at IITKGP	The procurement of instruments may be delayed by tendering delays. The IITKGP Seal Lab has world class expertise in this field – so they can deliver such a lab set up – but whether they can handle it at scale will be a question of limited hiring opportunity of engineers capable of these technologies
Machine Learning Based Malware Analysis tool	Tool developed needs to be robust, must work in sandbox, and sandbox must be connected to data-diode to prevent any harm to the system being protected while analyzing the malware using dynamics analysis or memory forensic techniques – so design and implementation must be robust and continuously improved
Honeypot Technology for CI-CPS and Dashboard for threat analytics, deployment and monitoring of honeypots	The risk is to build honeypots with data diode-based protection of the actual operational technology else, the attacker may exploit vulnerabilities in the honeypot platform and escape into the real infrastructure. The other risk is skill set shortage – which needs to be managed by sufficient research and training to create the skillset within the TIH
Machine learning based Anomaly detection for detecting Intrusion in Cyber Physical Systems	The risk again the shortage of skilled man power in developing this technology. Also, the machine learning methods always has false positives and false negatives. For skill set shortage, we must create the workforce through the TIH research and training programs. For the false positive and false negative problem, on-line learning to continually improve the models is our approach.
Cyber Asset Management Framework, and Console	The patch management in a critical infrastructure has multiple risks. First, in past attacks, stolen digital certificates were used to authenticate a patch, leading to patching PLCs with malware laced patches. Second, the patch may lead to compromise in functionality – hence requires a test-bed to first try the patches out. Third, the patch management must be properly recorded as unauthorized patches could indicate insider attacks.
Secure Operating System Distribution	Risk is there in terms of security guarantees as it is not possible to formally verify the security guarantees for a complex system as an OS. In fact, even if parts are formally verified which we plan to do – there is always a chance of vulnerabilities in other components. So it is a best-effort security.

16 Outcomes

Success of the Hub should be measured against the promised outcomes. The promised outcomes along with success measurements are provided below.

S No	Activity	Target	Success Measurement
1	**Technology Development**		
	(a) No of technologies developed	50	Deployment by users and licensing by industries
	(b) Technology products	50	
	(c) Publications, IPR and other intellectual activities	90	Appearance in journals, conferences, and as patents
	(d) Increase in CPS research base	105	Number of projects awarded to various research groups across the country
2	**Entrepreneurship Development**		
	(a) CPS Technology business incubator	1	*Already existing as a Section 8 company at IIT Kanpur*
	(b) CPS Startup and spinoff companies	125	Registration of startups in IITK Incubation Center
	(c) CPS Grand Challenges and Competition	4	Number of participants
	(d) CPS PRAYAS	1	Number of participating entrepreneurs
	(e) CPS Entrepreneur-in-residence	100	Number of startup founders at IITK incubation center
	(f) CPS Dedicated Innovation Accelerator	1	Number of startups availing accelerator program and their market value after three years
	(g) CPS Seed Support System	1	Number of startups availing seed fund
	(h) Job creation	13125	Number of additional jobs created through technologies developed at the Hub
3	**Human Resource Development**		
	(a) Graduate fellowships	360	Number of undergraduate students supported
	(b) Post graduate fellowships	110	Number of masters students supported
	(c) Doctoral fellowships	45	Number of PhD students supported
	(d) Faculty fellowships	20	Number of young faculty supported
	(e) Chair Professors	10	Number of senior faculty supported
	(f) Skill development	1000	Number of trained professionals through the Hub
4	**International Collaboration**		
	(a) International collaboration	4	Number of active collaborations with institutions outside India

Year-wise division of deliverables is given in the table below.

S No	Activity	Target	First Year	Second Year	Third Year	Fourth Year	Fifth Year
1	**Technology Development**						
	(a) No of technologies developed	50	5	10	10	10	15
	(b) Technology products	50	5	10	10	10	15
	(c) Publications, IPR and other intellectual activities	90	15	15	20	20	20
	(d) Increase in CPS research base	105	42	42	21		
2	**Entrepreneurship Development**						
	(a) CPS Technology business incubator	1	1				
	(b) CPS Startup and spinoff companies	125	15	25	25	30	30
	(c) CPS Grand Challenges and Competition	4	1	1	1	1	
	(d) CPS PRAYAS	1	1				
	(e) CPS Entrepreneur-in-residence	100	10	20	20	25	25
	(f) CPS Dedicated Innovation Accelerator	1	1				
	(g) CPS Seed Support System	1	1				
	(h) Job creation	13125	125	1000	3000	4000	5000
3	**Human Resource Development**						
	(a) Graduate fellowships	360	72	72	72	72	72
	(b) Post graduate fellowships	110	22	22	22	22	22
	(c) Doctoral fellowships	45	9	9	9	9	9
	(d) Faculty fellowships	20	8	4	4	4	
	(e) Chair Professors	10	4	2	2	2	
	(f) Skill development	1000	200	200	200	200	200
4	**International Collaboration**						
	(a) International collaboration	4	4				

17 Evaluation

The hub is creating internal review processes to evaluate its progress at regular intervals.

For Startups, evaluation process has been started on monthly basis by each of their respective portfolio managers and reports are to be submitted to the senior management for further evaluation and feedback.

For R&D projects, the progress will be monitored quarterly. The performances of all employees will be evaluated by their respective managers half-yearly.