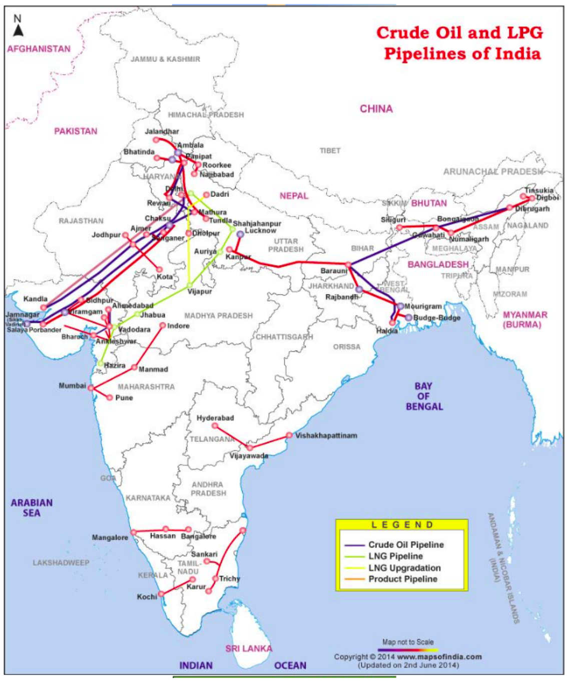
DETERRENCE OF CYBER ATTACK ON INDIAN OIL

Abu Shahid, 2022

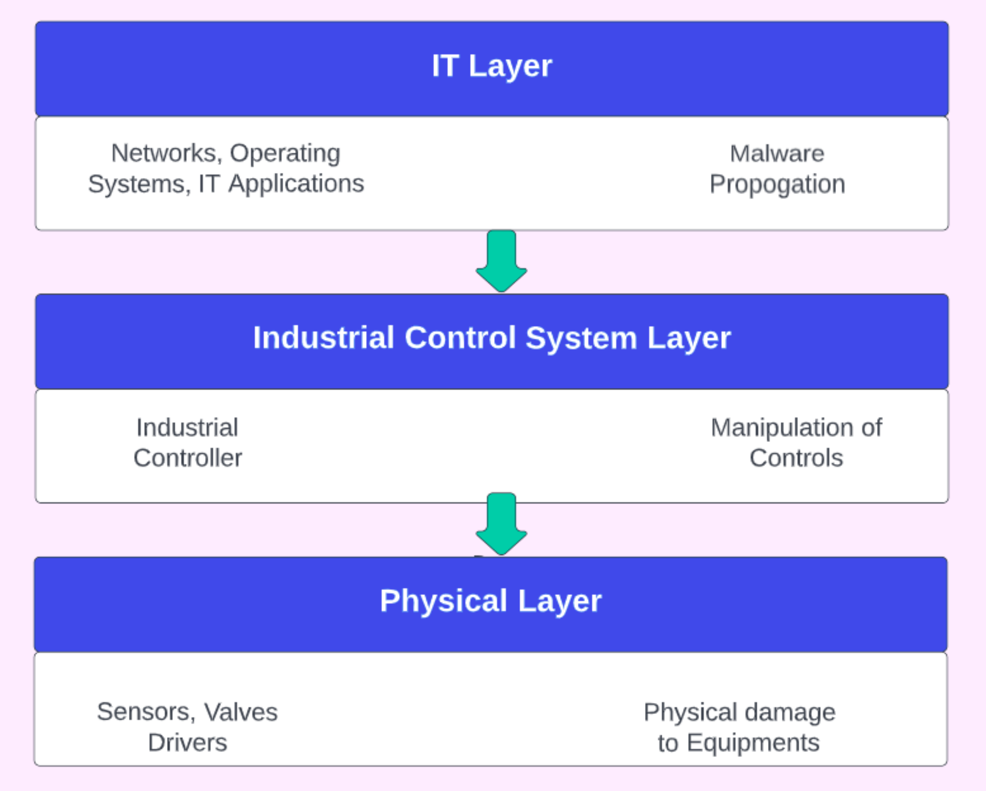
ABSTRACT: As part of this research paper, the author will attempt to go through the cyber security infrastructure at Indian Oil and devise a procedure to deal with the possibility of a Stuxnet kind of attack. IndianOil operates crude oil, petroleum product, and gas pipeline network that spans more than 15,000 kilometers and has a throughput capacity of 94.56 million metric tonnes per year of oil and 21.69 million metric standard cubic meters per day of gas. IndianOil, a pioneer in the country's oil pipelines and manager of one of the world's largest oil pipeline networks, reached a throughput of 76.019 million metric tonnes in 2020-21. With over 7 business divisions, in this paper, we will be going through their: **Refineries Division** and **Pipelines Division**. Clearly, any disruption in the supply chain is severely going to affect the entirety of the nation.



CONTENTS

I. METHODOLOGY AND ASSUMPTIONS

Overview of Industrial Control Systems at Indian Oil



Cyber-Physical Attack Layers

Here we would like to give special emphasis on Industrial Control System Layer. ICS are computerized components that control industrial processes. At Indian Oil, this is done through four basic steps. The *first step* is taking an accurate measurement of the status or condition of a process. The *second step* involves a controller evaluating potential actions to affect the process after considering that measurement and comparing it to the system's programmed optimal functioning values. The *third step* is the controller sending an output signal to alter the process based on the controller's evaluation of the measurement.

The resulting *fourth and final step* is the reaction to that output signal that manipulates the process itself toward optimal efficiency.

Critical Infrastructure(CI) ICS can be categorized into one of three categories that are extensively used. **Programmable logic computers (PLCs)**, **distributed control systems (DCSs)**, and **supervisory control and data acquisition (SCADA) systems** are the three main kinds.

1. For the IT layer of both the divisions, we are going to assume that the systems use a Windows operating system(7/ 8/ 10 /11*) or a Linux Distribution.
    a. They use some sort of firewall and anti-virus for protection.
    b. Sensitive systems are configured more rigorously.
2. ICS uses PLC. For our case we will go through the following PLCs which will be using the SCADA communication system:
    a. S7-300 (Siemens)
    b. S7-1200 (Siemens)

Apart from this, we assume they have suitable firewall IDSs and SIEMs. (their specific assumptions will be discussed in solution architecture).

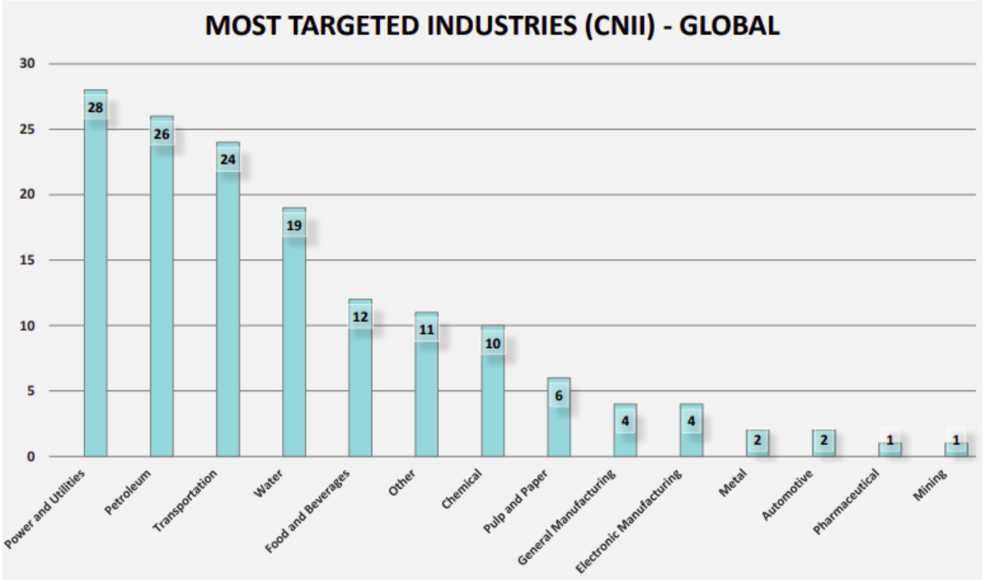
A rough outline of our proposed methodology

We here are making a notable assumption that budget and manpower is not a constraint.

Physical and cyber attacks on infrastructure must be included in plans, as well as the procedure for defending, mitigating, and responding to them. Today's supply chain is becoming increasingly complex and externalized as a result of substantial outsourcing, posing extra hazards. A supply chain's resilience is established by its weakest link, and operators are only safe if their entire network of partners and vendors is safe. Adversaries can jeopardize important operators by using partners who aren't well-protected. Business planning, contracts, and operations must all contain an integrated and long-term supply chain security goal. A policy of **Zero Trust** should be followed.

II. CYBER DETERRENCE CHALLENGES

According to a recent INTERPOL report, the Covid -19 pandemic has seen attacks migrate from small enterprises to critical infrastructure, government, and major corporations.



- Many critical infrastructure technologies are based on legacy IT and OT systems which are poorly secured, posing serious risks to utilities, and ultimately national security.

- Physical redundancies may be abandoned in the future as reliance on virtual infrastructure in the industry grows acceptable, making it easier for an attacker to carry out a severe breach that can inflict real damage.
- Hackers will put more effort into exploiting weaknesses as industries become more reliant on mobile devices and IoT devices.
- Rogue mobile apps that imitate well-known businesses but are meant to steal personal information are becoming more common.
- Every day, more gadgets are connecting to the internet, but there are no effective laws or governance in place, allowing countless loopholes to be exploited.
- Device security, data security, and the protection of individual privacy are all challenges in cybersecurity.
- As business demands for real-time data and interconnected networks become the norm, traditional air gaps used to protect control systems through separation are disappearing.
- Because attribution is difficult, verification is difficult. An intelligent adversary can obfuscate its actions by routing assaults or exploitations through anonymous computers all around the world. Even if one knows which computer in the world is responsible for an assault or exploitation, this information does not reveal who, or even which country, is behind the aggression.

III. LEGAL AND TREATY ASSUMPTIONS

The prospect of mutual gain is one of the requirements for a treaty, at least among powerful states. There is no motivation to enter into the legal contract/treaty or to follow it if there is no motive to do so. Even assuming that the large verification hurdles can be overcome, it is not obvious that a mutually beneficial contract is achievable in theory for most cybersecurity issues. Similarly, fundamental disagreements exist between countries regarding the value of intellectual property protection, freedom of speech and access to information, the nature and degree of necessary security carve-outs, state control over the network, and much more. These differences are difficult to reconcile.

Dealing with friendly states: Attribution can be a really difficult task. However, if the source of the attack is in a state friendly to India, talks can be set into motion through the Ministry of External Affairs and Ministry of Home Affairs. Existing Extradition Policy between the two states can be honored. Assistance can be sought from the accused country's National Cyber Law Enforcement body. In most the cases there might be an already existing treaty with the friendly nation

- In April 2017, Australia and India signed a Memorandum of Understanding concentrating on counter-terrorism and civil aviation security.
- A pre-existing Memorandum of Understanding (MoU) between Qatar and India, signed in December 2016, was added to the mapping. The agreement concerned a protocol for technological collaboration in cyberspace and cybercrime prevention.
- In March 2017, India and the United States signed a new Memorandum of Understanding. CERT-In and CERT-US signed a Memorandum of Understanding

> (MOU) committing to develop tighter cyber security cooperation and information sharing in accordance with applicable laws, rules, and regulations, and on the basis of equality, reciprocity, and mutual benefit.

The list goes on….

Dealing with neutral states: If the attack vectors originated from a neutral state, they can be asked to cooperate in the investigation as per international treaties like **Budapest Convention on Cybercrime.** A new Treaty and/or Extradition Policy can be signed if the other country meets our terms.

Dealing with hostile state: In the case of a hostile nation attacking our infrastructure, an ad hoc committee should be made comprising not only cybersecurity experts but also people from the background of External Affairs. In such cases, as there is no scope of cooperation from the enemy state, a proposal to retaliate with the means necessary can also be thought of. On the international front, India can ask other countries with vest the same interest as India to impose sanctions on the enemy state. Attack on an organization like Indian Oil, in this case, can have only one purpose- to destabilize the socio-economic state, even though it may be veiled like ransomware. Such an act should be seen as an act of cyberwar and appropriate measures should be taken; best formulated by the ad-hoc committee. This will heavily depend on the enemy state in question.

Dealing with domestic culprits: Domestic acts of Cyberviolence come under IT Act 2000, Indian Penal Code, Companies Act, 2013, and NIST Compliance. Further into IT Act:

- **Section 43** - This section applies to those who destroy computer systems without the owner's authorization. In such instances, the owner is entitled to full recompense for the total loss.
- **Section 66** - This section applies if a person is found to have committed any of the acts listed in section 43 dishonestly or fraudulently.
- **Section 66B** - Incorporates the penalties for receiving stolen communication devices or computers in a dishonest manner, which confirms a possible three-year sentence.
- **Section 66C** - This section looks into identity thefts including impostor digital signatures, password hacking, and other unique identification elements.
- **Section 66 D** - This section was added on the spot to focus on punishing cheaters who use computer resources to impersonate others.

IV. SOLUTION ARCHITECTURE

Organizations find it challenging to secure their ICS because of legacy systems. This has to do with how differing security priorities are maintained in IT and OT contexts. But in the current landscape of developments, a paradigm shift is being witnessed. As a part of this paper, we would like to be majorly concerned about the ICS layer and IT layer to some extent.

Solution Architecture for IT Layer

IndianOil being the country’s largest oil and gas company has a lot of stakeholders. They follow every update from the company. Any speculation about an accident or a rumor can throw the market into turmoil, even if the industrial systems remain completely intact and functional. A very similar scenario was seen in the case of the Colonial Pipeline hack where the organization fell for a ransomware attack and it took weeks to achieve normalcy. This shows the urgency to secure the IT circle of an organization especially if it is as critical as Indian Oil.

Keeping their network safe is not as simple as throwing up a firewall and using some anti-virus software. We will be going through various steps to secure our most exposed and superficial layer.

1. **Configuring Firewalls, IDS and IPTables:**

The various components within the IT layer should be bifurcated and placed on the fringe ranging from casual at one end to critical at the other. Suitably configured firewall should be set up in between them. More generally, for critical components, **stateful and application-based firewalls** should be used while for casual systems, **stateless and network** alternatives can be implemented.

Usage of IDS, even if configured properly, can lead to false positives as it is difficult to define normalcy. Here, a detailed trade-off analysis is needed and can subsequently be used for intrusion detection in more critical components. **A note must be taken to place Network IDS in machines that do not have an address.**

Static ARP tables must be used to prevent ARP Spoofing. In more important and critical sections, the default policy of the IP tables should be set to **DROP.**

2. **Setting up traffic thresholds:**

With a few more technical security measures, we can somewhat reduce DDoS attacks. Setting traffic thresholds and constraints, such as rate-limiting on our router and packet filters on dubious sources, among other things. As a first stage of mitigation, we can use lower SYN, ICMP, and UDP flood drop thresholds, IP backlisting, geo-blocking, and signature identification.

3. Securing Human Layer

When it comes to cybersecurity, people are, without a doubt, the weakest link in practically every regard. Putting in place a regular education programme to teach staff about the benefits of good cybersecurity behaviors can greatly lower the chances of a successful assault. This covers advice on how to recognize a phishing effort, how to create strong passwords, and current scams to be aware of. Access constraints are also a smart concept for securing the human layer since they limit the amount of harm that can be done if an attack is successful.

Apart from all this, the organization should also have a mechanism for data inventory and data segregation set in place.

Solution Architecture for ICS Layer

The following are the strategies for strengthening the utility security of the Industrial Control System:

1. Enforcing encryption of sensitive data and limiting the usage of USB media and other portable storage devices.
2. Air gap control system networks where possible, and use specific firewalls and/or one-way data transfer devices to restrict connection points to other networks.
3. Using a specialized version control system for control system/PLC code, that enables version control and reversion to a recognized good version when unusual behavior happens after a modification.
4. Implementing mechanisms for message integrity validation and source verification.

1. Risks and Mitigation Techniques for Portable Storage Media

Sensitive infrastructure should not allow the employees to use USB devices. If at all one is needed, there should be a series of sandboxing and detonation attempts. While prohibiting the use of USB storage devices eliminates one threat vector for isolated networks like air-gapped control systems, portable storage media remains one of the only ways to transfer data between physically separate networks.

- Using **WORM** (write-once, read-many) storage for backups is one way for reducing the risk of portable storage media. Data on essential assets might be burned to DVDs using one or more computers on the control system network, and then the backup DVDs could be taken off-site for storage.
- A further option for reducing the hazards associated with USB storage media is to do a low-level format of all USB drives on a standalone machine running a bootable operating system like Knoppix Linux. Once a USB or CD/DVD has been generated from an ISO image downloaded from a trusted/known good source repository, the ISO can be checked for tampering using an **MD5 or SHA-1** checksum. The system can then be trusted to format portable USB memory devices such as a hard disc and/or a flash memory stick/thumb drive when booted from a disc or USB drive that was likewise formatted fresh before being made bootable. After formatting, the device(s) can be used on control system computers with the assurance that all possible dangers posed by portable storage media have been mitigated.

2. Modern Network Infrastructure and Air Gaps

Air gaps have been used as a security precaution for decades to secure systems and devices by isolating them from other systems and/or networks. Compromise of mission-critical software and/or hardware required for the uninterrupted supply of utility services can be caused by network-borne and/or Internet-based threats. While an air-gapped network is preferable for the benefit of physical separation from other Internet-connected devices and networks, the challenge of having insight into operations and executing routine system maintenance duties, as previously indicated, becomes problematic.

3. Securing Control Systems in a Networked Environment

The usage of unidirectional security gateways is one option for permitting network connectivity while avoiding danger. These devices act as a one-way firewall, letting data flow from one network's approved sending devices to one or more networks' allowed receiving devices. Allowing control system computers to download Windows operating system patches from a Microsoft Webserver on the business network, for example, after necessary testing and validation to ensure the upgrades do not damage SCADA applications has been completed.

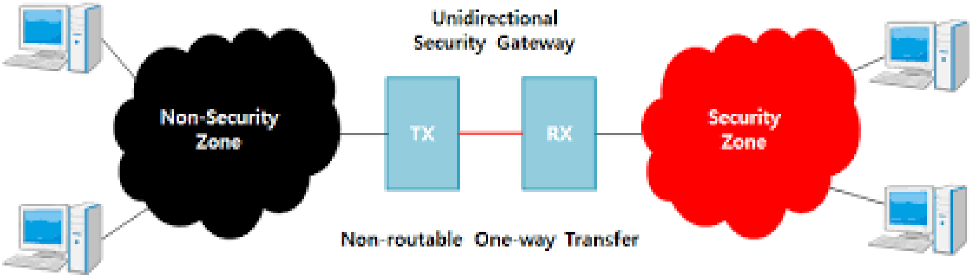

Unidirectional Security Gateway
Non-Security Zone
TX
RX
Security Zone
Non-routable One-way Transfer

Diagram Courtesy

Having such a unidirectional gateway can have the following far-reaching effects:

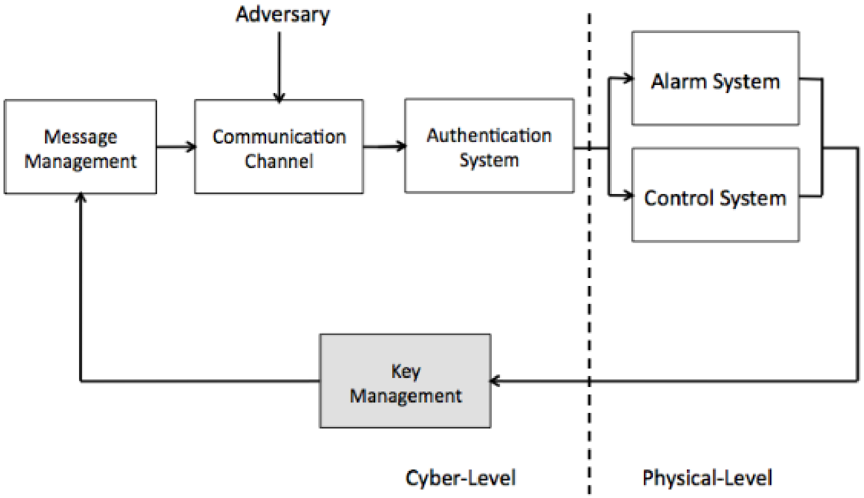
- **Complete Protection Against External cyberattacks-** Hacking sessions are an interactive effort. The hacker will be unable to begin a successful session when attempting to hack via a unidirectional gateway.
- No data backflow.
- **Non-routable protocols-** It is not possible to use a communication path to send messages or information to unintended or unplanned destinations.

4. **PLC Signal Authentication using randomized set of cryptographic keys**

In one of the stages of the attack, Stuxnet used to monitor the PLC readings for 21 seconds and used to replay it to SCADA as long as the attack was underway. With no policy to verify the integrity of messages, no alarm used to be raised.

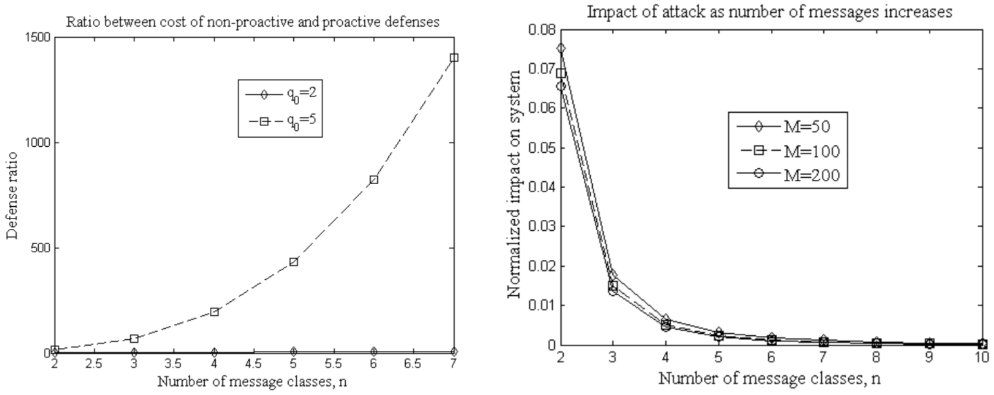
- A system architecture for securing communications between a system operator and PLCs is proposed. We consider both the cyber and physical elements of the problem, such as authentication of control messages to PLCs and the damage caused by unauthorized messages on ICSs.

Under this, we propose a **System and Adversary Model.**



The model is made up of six components. A workstation operator transmits messages to PLCs across a potentially vulnerable communication route. Message management classifies messages into many categories, including phony messages meant to deceive the enemy. The messages can be classified into **n classes utilizing K keys.**

The defense gain, defined as the difference between the impact of an attack with non-proactive and proactive defenses, increases exponentially with key length and polynomially with the number of message classes.



Courtesy [3]

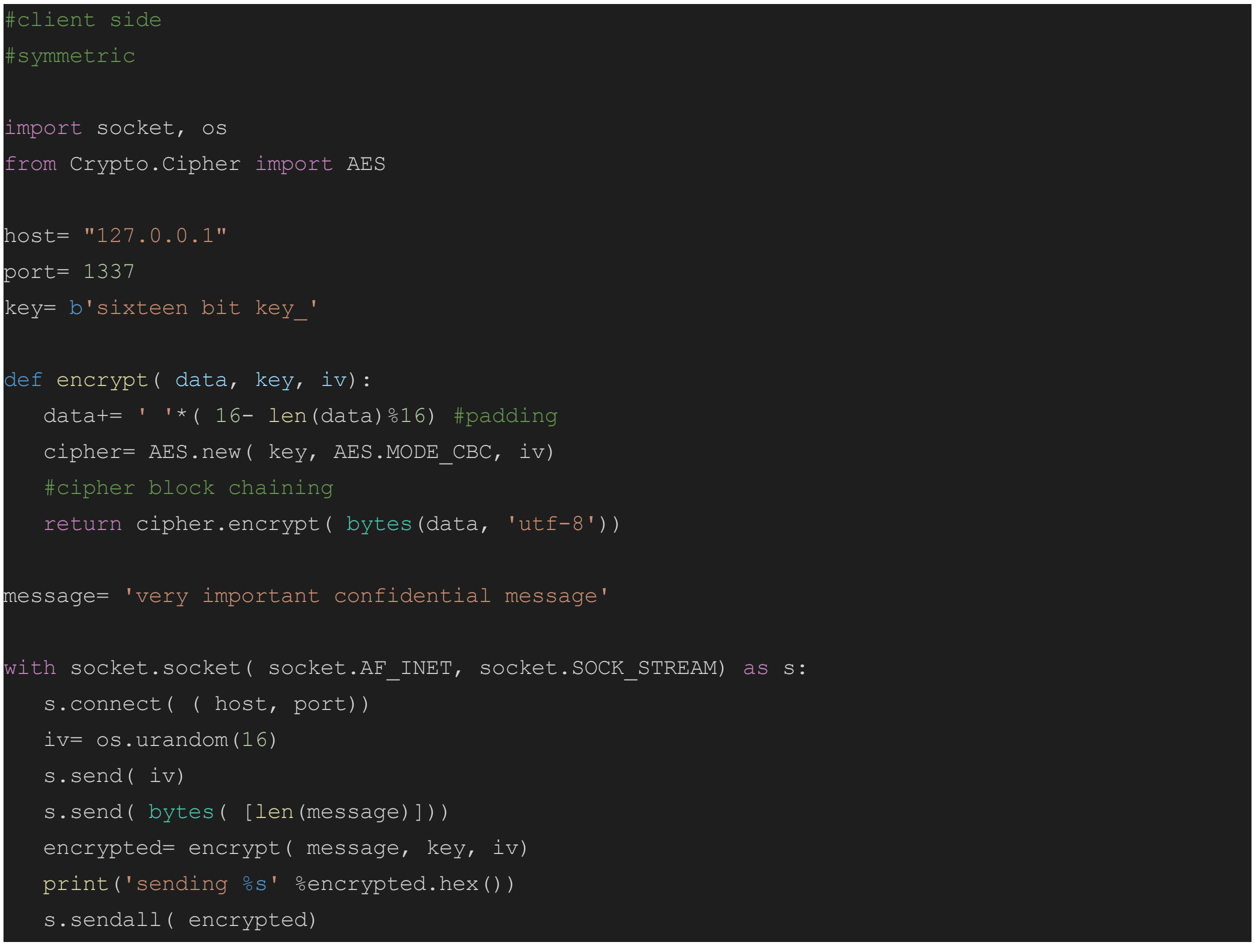
V. PROTOTYPE

Code files for the same can be found at the Github repo: ceyxasm/cybersecurity_engage

1. Encrypted Communication

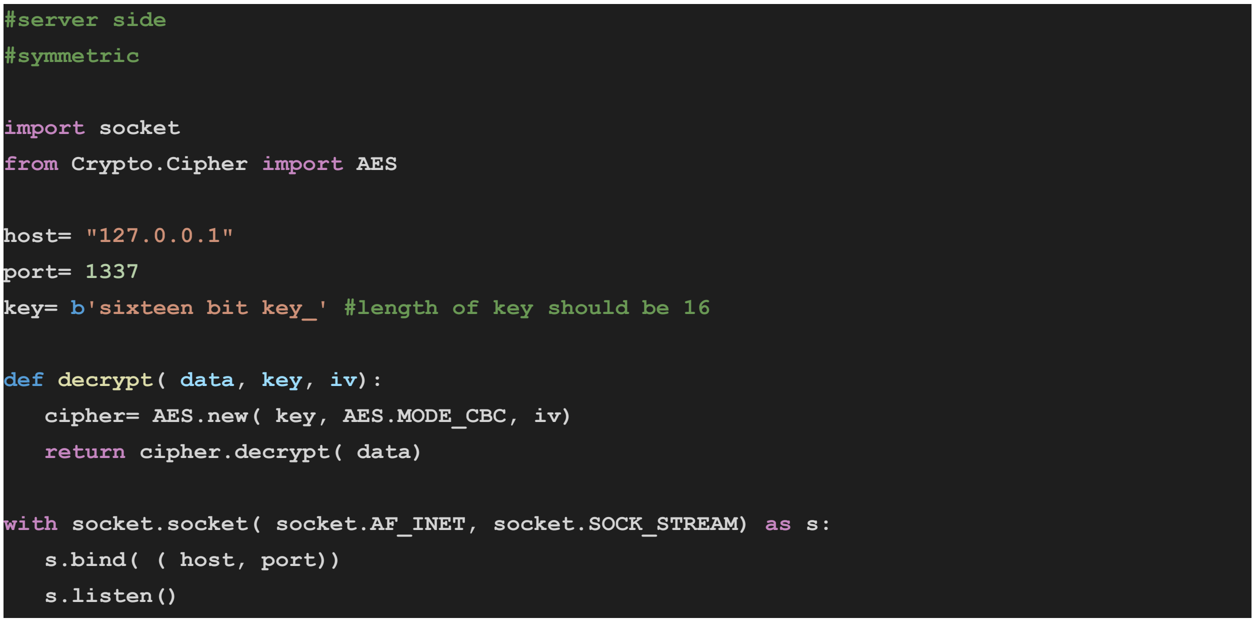
As discussed in solution architecture, we need to enforce the encryption of sensitive data. Below is the code to set up an encrypted channel using AES encryption.

Client Side

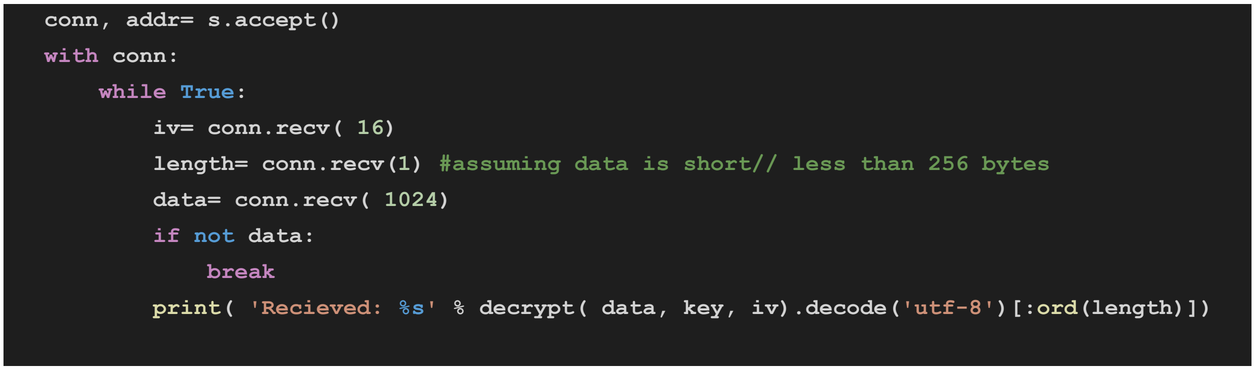


```
#client side
#symmetric

import socket, os
from Crypto.Cipher import AES

host= "127.0.0.1"
port= 1337
key= b'sixteen bit key_'

def encrypt( data, key, iv):
   data+= ' '*( 16- len(data)%16) #padding
   cipher= AES.new( key, AES.MODE_CBC, iv)
   #cipher block chaining
   return cipher.encrypt( bytes(data, 'utf-8'))

message= 'very important confidential message'

with socket.socket( socket.AF_INET, socket.SOCK_STREAM) as s:
   s.connect( ( host, port))
   iv= os.urandom(16)
   s.send( iv)
   s.send( bytes( [len(message)]))
   encrypted= encrypt( message, key, iv)
   print('sending %s' %encrypted.hex())
   s.sendall( encrypted)
```

Server Side



```
#server side
#symmetric

import socket
from Crypto.Cipher import AES

host= "127.0.0.1"
port= 1337
key= b'sixteen bit key_' #length of key should be 16

def decrypt( data, key, iv):
   cipher= AES.new( key, AES.MODE_CBC, iv)
   return cipher.decrypt( data)

with socket.socket( socket.AF_INET, socket.SOCK_STREAM) as s:
   s.bind( ( host, port))
   s.listen()
```



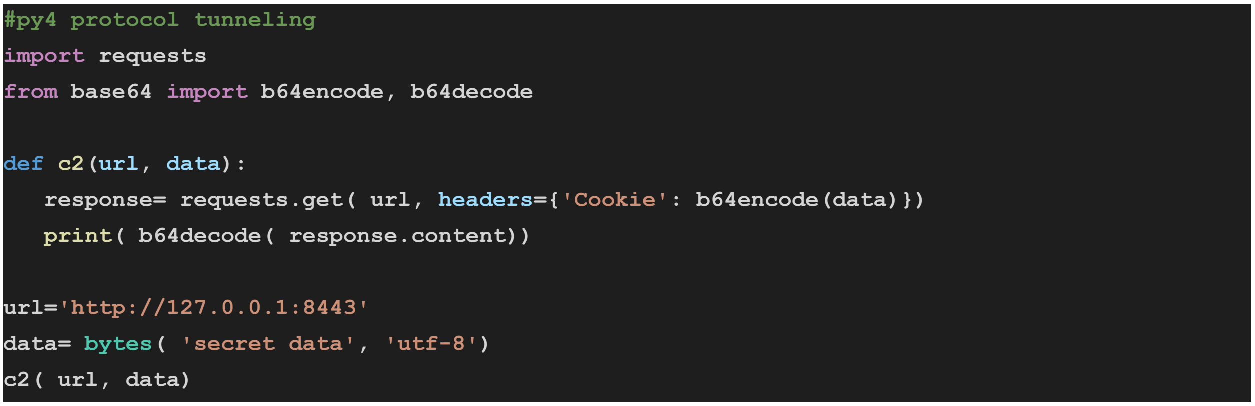
```
    conn, addr= s.accept()
    with conn:
        while True:
            iv= conn.recv( 16)
            length= conn.recv(1) #assuming data is short// less than 256 bytes
            data= conn.recv( 1024)
            if not data:
                break
            print( 'Recieved: %s' % decrypt( data, key, iv).decode('utf-8')[:ord(length)])
```

2. *Integrity Testing*

a. Integrity Against Protocol Tunneling:

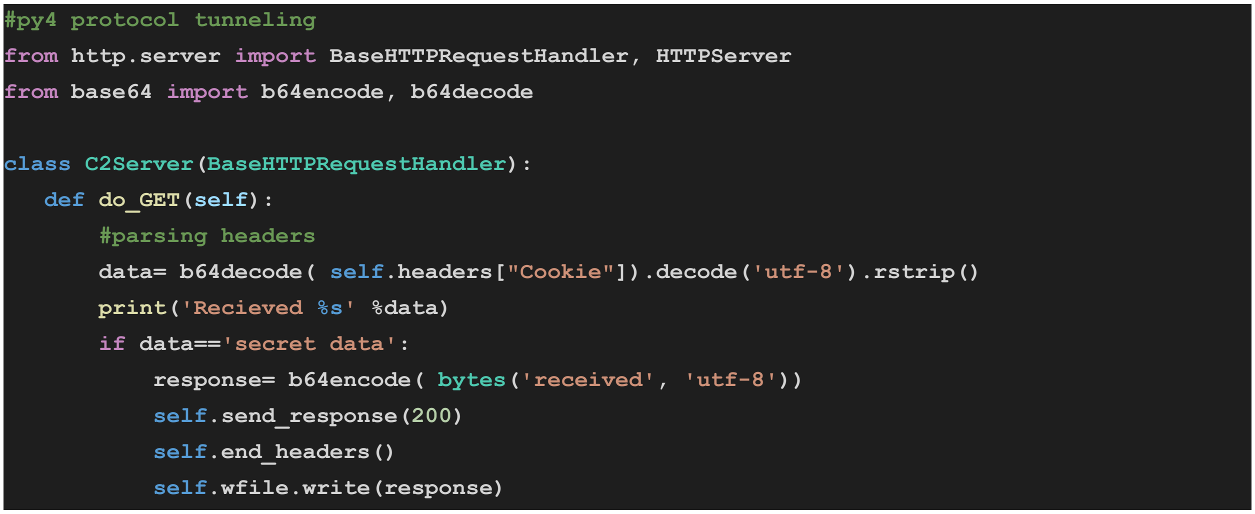
Our system architecture should red flag an attempted protocol tunneling. Following is the code to perform protocol tunneling.

Client-Side

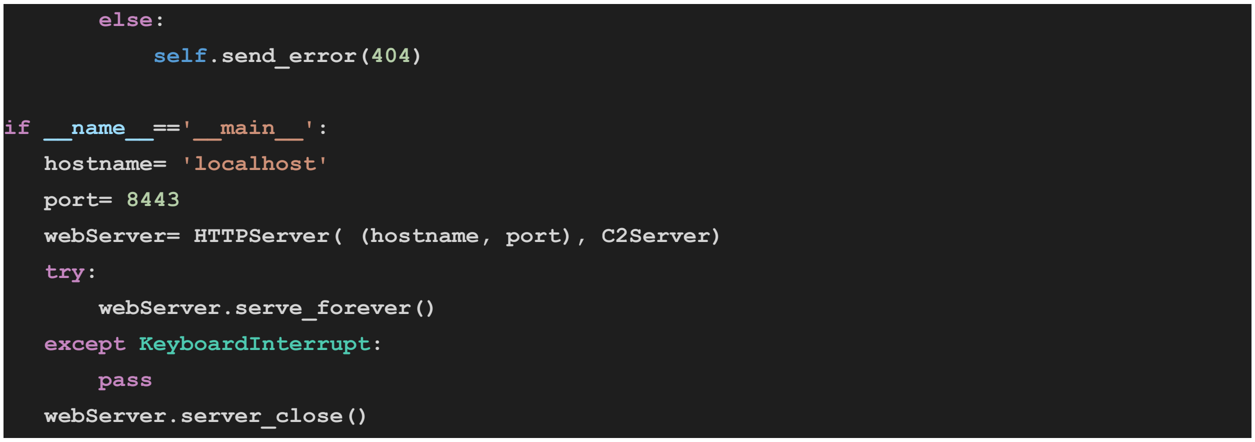


```
#py4 protocol tunneling
import requests
from base64 import b64encode, b64decode

def c2(url, data):
    response= requests.get( url, headers={'Cookie': b64encode(data)})
    print( b64decode( response.content))

url='http://127.0.0.1:8443'
data= bytes( 'secret data', 'utf-8')
c2( url, data)
```

Server Side



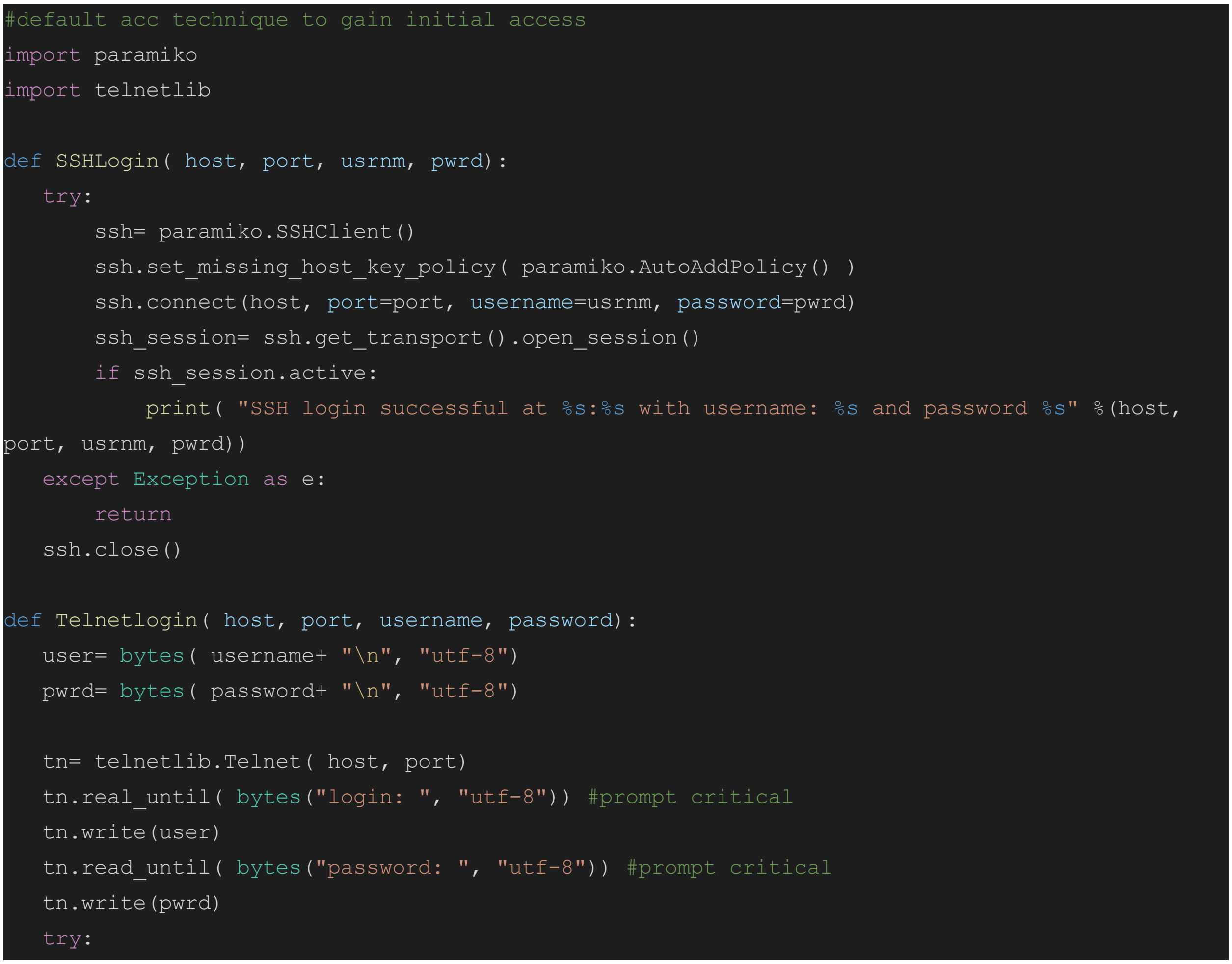
```
#py4 protocol tunneling
from http.server import BaseHTTPRequestHandler, HTTPServer
from base64 import b64encode, b64decode

class C2Server(BaseHTTPRequestHandler):
    def do_GET(self):
        #parsing headers
        data= b64decode( self.headers["Cookie"]).decode('utf-8').rstrip()
        print('Recieved %s' %data)
        if data=='secret data':
            response= b64encode( bytes('received', 'utf-8'))
            self.send_response(200)
            self.end_headers()
            self.wfile.write(response)
```



```
        else:
            self.send_error(404)

if __name__=='__main__':
    hostname= 'localhost'
    port= 8443
    webServer= HTTPServer( (hostname, port), C2Server)
    try:
        webServer.serve_forever()
    except KeyboardInterrupt:
        pass
    webServer.server_close()
```

b. Integrity Against Default Credentials:

A routine inspection must be performed to ensure that none of the systems are using default credentials. Code for the same.



```
#default acc technique to gain initial access
import paramiko
import telnetlib

def SSHLogin( host, port, usrnm, pwrd):
    try:
        ssh= paramiko.SSHClient()
        ssh.set_missing_host_key_policy( paramiko.AutoAddPolicy() )
        ssh.connect(host, port=port, username=usrnm, password=pwrd)
        ssh_session= ssh.get_transport().open_session()
        if ssh_session.active:
            print( "SSH login successful at %s:%s with username: %s and password %s" %(host,
port, usrnm, pwrd))
    except Exception as e:
        return
    ssh.close()

def Telnetlogin( host, port, username, password):
    user= bytes( username+ "\n", "utf-8")
    pwrd= bytes( password+ "\n", "utf-8")

    tn= telnetlib.Telnet( host, port)
    tn.real_until( bytes("login: ", "utf-8")) #prompt critical
    tn.write(user)
    tn.read_until( bytes("password: ", "utf-8")) #prompt critical
    tn.write(pwrd)
    try:
        result= tn.expect( [ bytes( "Last login: ", "utf-8")], timeout=2)
        if result[0]>0:
            print( "Telnet login successful at %s:%s with username: %s and password %s" %(host,
port, usrnm, pwrd))
        tn.close()
    except EOFError:
        print("login failure")

host="127.0.0.1"
with open("defaults.txt", "r") as f:
    for line in f:
        vals= line.split()
        username= vals[0].strip()
        password= vals[1].strip()
        SSHLogin(host, 22, username, password)
        Telnetlogin( host, 23, username, password)
```

c. Performing Port Scan for vulnerabilities:

A routine port scan must be performed to make sure none of the ports are poorly configured.

```
from scapy.all import *
ports= [25, 80, 53, 443, 445, 8080, 8443, 21, 22, 110, 995, 143, 993, 26, 587, 3306,
            2082, 2083, 2086, 2087, 2095, 2096, 2077, 2078] #not exhaustive

def synScan(host):
    ans, unans= sr( IP(dst= host)/TCP(sport=5555, dport= ports, flags="S"), timeout=2,
verbose=0)
    print('open ports at %s' %host)
    for (s, r) in ans:
        if s[TCP].dport== r[TCP].sport:
            print(r[TCP].sport, ' ')

def DNSScan( host):
    ans, unans= sr( IP(dst= host)/UDP(sport=5555, dport= 53)/DNS(rd=1,
qd=DNSQR(qname="google.com")), timeout=2, verbose=0)
    if ans:
        print("DNS server at %s"%host)

# host='8.8.8.8'
host= '14.139.37.109' #gateway of iitj
# host= '8.8.4.4'
synScan(host)
DNSScan(host)
```

VI. BENCHMARKS FOR SUCCESS

To better gauge our preparedness and to keep the flow of funds for setting up the cyber security infrastructure, we need to define certain benchmarks for success for the policymakers and for our own analysis. These benchmarks can be grouped into one of the two categories:

- Protection Metrics
- Incident Metrics

We need to elaborate a persistent and reproducible risk management system for identifying, assessing, and responding to cybersecurity risks. Then these pointers can be analyzed statistically.

Protection Metrics

Protection metrics will be benchmarking success when there are no cybersecurity incidents or when possible incidents were averted. With our proposed architecture, incidents of DDoS and virus contamination are expected to go down. The organization can keep a log of all the incidents and the history can be statistically analyzed. Raising positive flags during procedures such as sandbox detonation or IP blacklisting can further boost this metric, making it apparent to the policymakers, the advantage of the proposed architecture. Constant monitoring of firewalls and Intrusion Detection Systems and reporting its trends can also help in presenting forth the utility of our architecture. An exhaustive list may vary from division to division but a general list can look like the following:

- IP Blocks per month
- Phishing attempts averted (per month)
- Anomalies detected (per month)

Incident Metrics

These metrics are to be reported when an attack is successful. With the architecture set in place, different divisions of Indian Oil will now be independent in theory. In case of an attack, the infection cannot spread from one division to another. So even in its early stages, the infrastructure is going through damage control. This also helps in reducing the downtime the system faces. Here, the data inventory and segregation steps we took earlier are going to be very useful in performing backups of data lost.

A non-exhaustive list of such metrics can be:

- Number of server downtimes.
- Average server downtime

Apart from these generic metrics, the detailed report provided by the cyberthreat analysis team after the attack is over will be better able to justify architectural decisions taken.

VII. REFERENCES

1. SHADOWS OF STUXNET: RECOMMENDATIONS FOR U.S. POLICY ON CRITICAL INFRASTRUCTURE CYBER DEFENSE DERIVED FROM THE STUXNET ATTACK
2. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems: Applied to Stuxnet
3. An Impact Awareness Against Struxnet
4. Mapping of India’s Cyber Security-Related Bilateral Agreements
5. Cybersecurity Treaties: A Skeptical View
6. Cybersecurity: Safeguarding Networks
7. Safeguarding Critical National Information Infrastructure
8. All you need to know about Cybersecurity Laws in India