International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Evolution, Working and Solution to Security Threats in Virtual Data Acquisition Systems

Ayush Chaturvedi, Divyanshu Shekhar, Lakesh Goel, Gaurav Sharma, Harendra Kalyan

ABSTRACT: ***After the Industrial Revolution, big industries and factories came into being and the amount of information i.e. data increased tremendously and hence it became very difficult to keep track of them. Therefore, the need to have a system of database which can be used to keep track of the data that has variables of different types. The evolution of such data acquisition system is traced, the present system in practice is discussed and the future scope of improvement is realized. Today these systems are mostly web based so there is a big security threat which needs to be addressed. This paper highlights the existing solutions and proposes some unique methods to increase the security of Data Acquisition systems.***

Key-Words: Virtual Data Acquisition, Working and evolution of SCADA, Secure SCADA networks

I. INTRODUCTION:

The importance of virtual data acquisition system is quite evident from the fact that "Ours is a data driven world" and since this data not only helps in studying the systems well but also provides assistance in improving them. It is very difficult to keep an account of all the variables in the system physically. Hence, virtual data acquisition systems were developed and over the past decades it has undergone huge transformation.

II. EVOLUTION OF VIRTUAL DATA ACQUISITION:

On 2 December 1963, IBM launched its first data acquisition system named IBM 7700.It was an 18-bit system, capable of processing data from 32 sources simultaneously. Arithmetic instructions were processed in 2 to 3 machine cycles but for multiplication it was 8 and for division it was 12 in which one machine cycle was of 2 microseconds. It was capable of transmitting outputs to 16 remote printers, display units. The evolution of this invention goes back to 19 January 1960 when IBM announced 7080 data processing systems. It was able to communicate data over telephones at 150 characters per second. these were followed by IBM 7074 which had twice as fast processing speed as IBM 7070. It introduced IBM 1418 optical character reader which can read typed information from paper and cards.

Manuscript received on April 04, 2020.
Revised Manuscript received on April 25, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Ayush Chaturvedi*, Department of Electrical and Electronics Engineering Maharaja Agrasen Institute of Technology
Divyanshu Shekhar, Department of Electrical and Electronics Engineering Maharaja Agrasen Institute of Technology
Lakesh Goel, Gaurav Sharma, Department of Electrical and Electronics Engineering Maharaja Agrasen Institute of Technology
Harendra Kalyan, Department of Electrical and Electronics Engineering Maharaja Agrasen Institute of Technology

At the end of 1960, IBM product portfolio included IBM 7070,7080,7090,1401,1620 transistor data processing systems, IBM 704,705,709 large systems, IBM 1200 series character sensing equipment and IBM magnetic tapes transmission terminal and data transceivers. On 9 March 1961, IBM launched 1710 industrial control system which was capable to do various sampling and interpretation tasks in industries. Soon after IBM 1203 was launched which capable of performing automated demand deposits accounting. At the end of 1961 it launched HYPER TAPE which was the fastest data processing system at that time. These systems were designed on FORTRAN and COBOL. Various features were added in these systems with time which included automatically producing engineering designs of products like turbines, motor, generators, circuits, transformers, audio response units etc. The IBM 7404 graphical output unit could automatically plot full sized graphs, maps, diagrams from computer generated information. The IBM 1800 SYSTEM was able to monitor a whole assembly line, missile launch and manage business data.

A. History of supervisory control systems-

A.1 Pilot wire systems :

These were used to operate remote substations which used a pair of wires between the sites, with this serviced were restored rapidly.

A.2 Stepping switch systems:

In this they multiplexed one pair of wire so that they can use multiple sites which could increase their efficiency. But there were concerns over the security features, as any snag could make a huge damage. So, to rectify this they used select/check/operate method in which this three-part process was done at each level i.e. from master to remote location.

A.3 Relay systems:

They used telephone relays which created pulses that were transmitted through a communication channel.

A.4 *Redac*:

Another data acquisition system was developed by Westinghouse in early 1960s. It also used the select/check/operate technique in which they used a fixed word length with a checksum character with each message. General electric also used similar system which they named GETAC.

A.5 Telemetry:

Supervisory control systems required values of voltages, current, power factors to control the locations. This required a pair of wires which were used to transmit current proportional to readings.

They required transducers which could convert AC pulses into DC. They were called thermal converters. They used inputs from current and voltage reading to heat an element which was passed through a thermocouple to create the voltage, hall effect was also used in these systems.

A.6 Automatic data loggers:

In the earlier systems reading and storing the data manually from the systems from time to time was a very difficult and time consuming. This invention relieved the workload from workers by automatically storing the real time values.

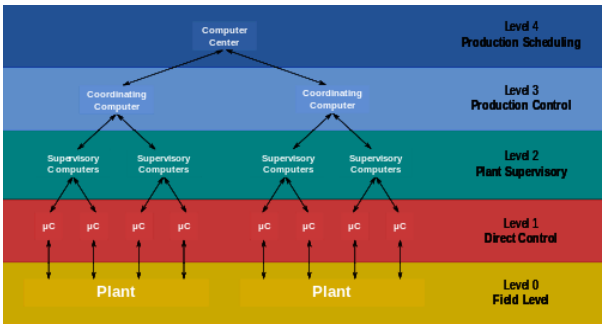
A.7 SCADA systems after 1970s:

By middle 1960s there were computers which were capable of doing real time functions. These included scanning data, monitoring the data, alarming for changes, CRT displays. In this only master could send the data and the remote would only respond SCADA stands for Supervisory Control and Data Acquisition system that works on a control system architecture that helps user data and information from multiple facilities and sends in restricted control instructions. It uses computers and related communication systems for supervisory control whereas discrete PID controller and Programmable Logic Controller (PLC) to interact with the plant or machines. It helps in monitoring and issuing process commands.

III. WORKING:

The working of the SCADA system can be understood using the following diagram:

(Ref.-Wikipedia)



(diagram to explain the working of SCADA)

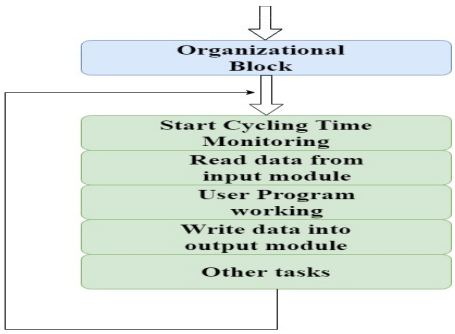
- Level 0 contains the field devices such as flow and temperature sensors, and final control elements.
- Level 1 contains the industrialized input/output (I/O) modules, and their associated, distributed electronic processors that will take in these inputs using RTUs and PLC.
- Level 2 contains the supervisory computers that helps in collecting the data associated with the system to be displayed or recorded.
- Level 3 is the production control level which is concerned with monitoring production and targets.
- Level 4 is the production scheduling level.

IV. REMOTE TERMINAL UNIT:

This was the nomenclature given to remote stations. RTU was a solid-state component made up of printed circuit boards and was installed in equipment cabinets. They were supposed to work even after the supply was off therefore, they were connected to a 129 V battery. They worked on BCH security codes which was common in the 1960s. Common protocols such as ASCII was not used. Today RTU can communicate with different protocols as microprocessor based communication interface can be programmed to handle different protocols.

V. PROGRAMMABLE LOGIC CONTROLLER:

PLCs are designed to work in harsh conditions which is composed of power supply, CPU, input / output memory, operating software. PLC are designed to perform discrete and continuous function which makes it different from a PC. The most important advantage of a PLC is that they can be programmed as per the current manufacturing needs. It can count, time, calculate various analog signals automatically. The working of PLC can be understood using the block diagram shown below



(block diagram of PLC)

VI. MAN MACHINE INTERFACE:

Earlier pushbuttons were used to give commands but later on cathode ray tubes improved the man machine interface. In the early 1980s graphical interface was added which allowed circuit diagrams to be designed and controlled through a monitor. A single mouse click could now change the circuits and made the manufacturing process more efficient.

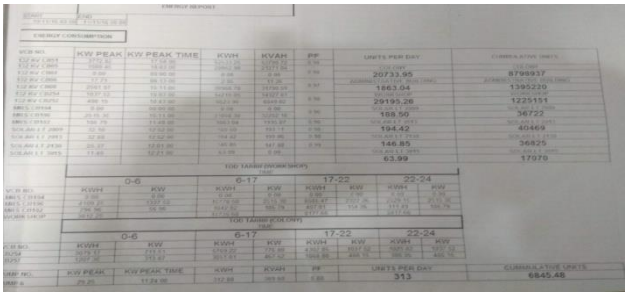
VII. COMMUNICATION CHANNEL:

Earlier a pair of communication media was used as a channel in which modem was provided by the vendor but later on power line carriers were used. In the late eighties microwave equipment were used which had an advantage to be able to communicate with different communication channels simultaneously.

VIII. OBSERVATIONS:

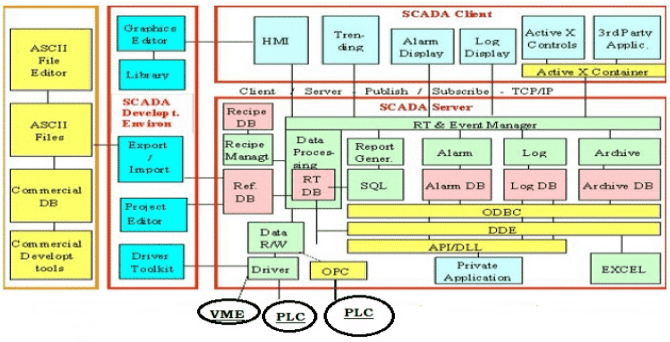
The SCADA system can produce daily expenditure cost report which is useful in the sense that many industries today buy electricity from the local electricity boards on a daily basis. With this they can improve the efficiency and costs of manufacturing, also they can have special provisioning in the circuits during the peak hours for protection.

One such model report is attached below to have a better understanding.



IX.SCADA ARCHITECTURE:

The basic architecture of SCADA is shown below which can be understood by classifying this into 4 broad categories.



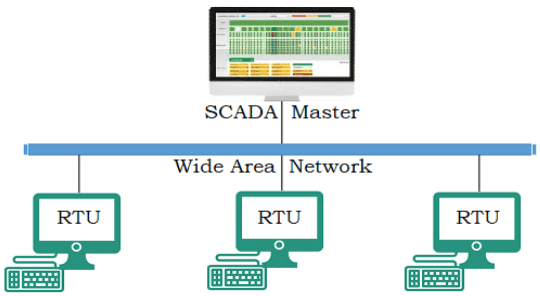
(diagram to explain SCADA architecture)

The architecture of SCADA can be broadly classified into four categories-

- Monolithic
- Distributed
- Networked
- Web based

A. Monolithic:

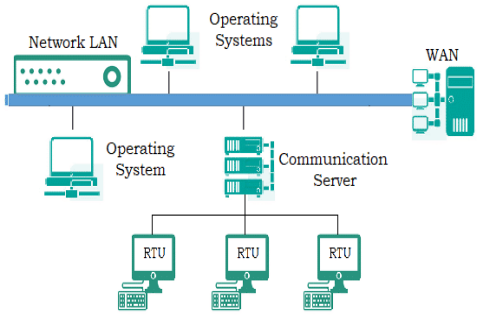
Earlier the SCADA systems were focused on mainframe computers due to which it wasn't able to communicate with other systems. The wide area networks were used such that it was able to communicate only with the RTUs. They were only able to scan and control circuit points in RTU. The interconnection between different RTU was not there with the master computer, which is shown below-



(monolithic network diagram)

B. Distributed:

In this system multiple systems can communicate with each other and can interchange the data. The size and cost of the computers in this generation is also less.

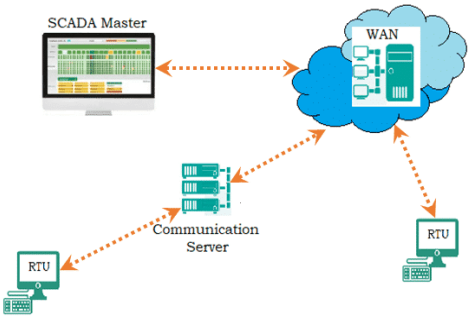


(distributed network system)

The above figure shows the distributed system which consisted communication processors, RTU, calculation processors, database servers.

C. Network systems:

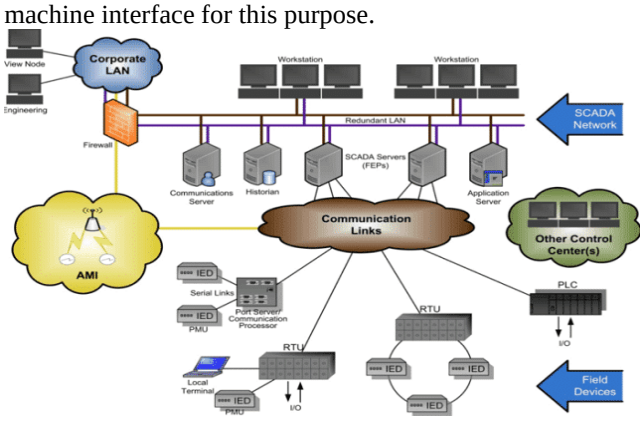
In the first two generations the vendor controlled the architecture, but in this generation open source architecture were introduced which allowed the SCADA to function in WAN instead of LAN due to its open and flexible protocol. This resulted in additions of various new features .For the data transmission fibre optic cables and ethernet were used which is shown below



(network system system)

D. Web-based:

This development allowed person to change, view, exchange the data from anywhere in the world, google chrome and Mozilla Firefox can easily be used as a human machine interface for this purpose.



(web-based system)

X. VULNERABILITIES in SCADA SYSTEM:

SCADA system is the heart and soul of the control of industrial and commercial operations in this modern and technology driven world. The advancement in technology also comes with susceptibility to malicious individuals, Belligerent nations, terrorist groups, curious hackers, and etc. In a related article, "The Truth About Cyber Terrorism," in the same issue of CIO magazine, Berinato further states that "CIOs and security experts are beginning to challenge the assumption that a hack on the nation's critical infrastructure will be the next big terrorist outrage. In fact, cyber terrorism may not be nearly as worrisome as some would make it. That's because it is utterly defensible. Since SCADA was developed in the non-internet era, it was rendered secured. But with the advent of the World Wide Web it became easier for hackers and foreign intruders to crack. There have been a series of events around the world that serve as proofs to the loopholes that exist in the system. The major risk elements to SCADA systems can be summarized as follows:

- Connections to additional, possibly vulnerable networks.
- Using standard hardware platforms with known vulnerabilities.
- Using standard software with known vulnerabilities.
- Other vulnerable remote connections.
- Real-time deterministic requirements in contrast to information security controls that might cause delays.

It is very important to access these risk elements existing in the system and provide a solution for a more robust system. It is high time we mitigate such problems in the system to render our industries and fellow beings safe and secure.

VULNERABILITIES	THREATS
OT systems run on legacy software that lack sufficient user and system verification.	Some firewall features fail to detect or block malicious activities.
Simple passwords and default configurations make systems vulnerable for attacks.	Invalidated sources, limited access allow the hackers to sabotaging OT systems to execute attacks.
If the SCADA software lacks necessary encryption, hackers can use sniffing software to get the username and password.	Traditional systems having PLCs and human man interface are connected to web networks which are vulnerable to cross site scripting and SQL injection attacks.
Systems which are connected to remote access servers are prone to backdoor access by hackers.	Scada systems should have anti malware protection, patch management policies and host-based firewall controls for security.

XI.EXISTING SOLUTION OF SCADA SYSTEM:

Existing solution of SCADA system is usage of IDS (Intrusion Detection System) and IPS (intrusion prevention system). Intrusion Detection System: SCADA system use two of IDS-

A. Network Base
B. Signature Base
C. Firewall
D. Host Base Security

A. Network Base IDS:

A network-based IDS captures and evaluates message packets traveling over a network segment. These IDSs are typically passive devices that use sensors to monitor network traffic and are designed to protect the host computers. In times of high network traffic, network-based IDS might experience problems in monitoring all the packets and might miss an attack being launched. Also, a network-based IDS cannot analyze encrypted packets and, therefore, cannot Identify an attack using encrypted messages. A third weakness of a network-based IDS is that, even though it can tell whether an attack was launched, it cannot determine the result of the attack. Thus, manual intervention is required to discern if the attack was successful against a network host.

B. Signature Base IDS:

A signature-based IDS, or misuse IDS as it is sometimes called, monitors system activity and compares the activity characteristics with characteristics or patterns of known attacks stored in a database. Because this type of IDS bases its alarms on matching a known attack pattern, it can provide specific information on the type of attack and generates less false positives than an anomaly-based IDS. A disadvantage of signature-based IDS is that it cannot detect new attack types that are not stored in the attack signature database. Therefore, the database must constantly be updated with patterns of new attacks. Also, in applying signature-based IDS to SCADA, the attack signature database will have different characteristics than signatures in an IT-oriented database. In particular, the signatures will have to be correlated with SCADA protocols such as Foundation fieldbus, Modbus, Profinet, ControlNet, and so on. Typical SCADA IDS signature components include IP addresses, transmitted parameters, and protocols.

C. Firewall:

Firewall is the basic and important part of security. Firewall help to monitor the ingoing traffic and outgoing traffic. So due to this fire wall act as a barrier between system and cyberworld. Firewall also blocks suspicious traffic.

In SCADA system too firewall act as an important part of Security SCADA system. Firewall provide basic security to the system.

D. Host Base Security:

Host base security involve manually checking log file. It vulnerable because if host misses any import log or by mistake delete any important log, it may create a problem for the system. So that as number of log increases probability of mistake increases. That's why this is the most vulnerable part of the existing security .

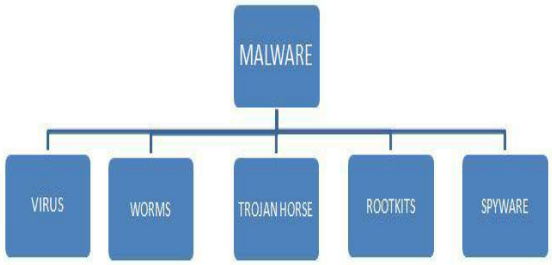
XII.PROPOSED SOLUTION:

The aim of the paper is to present a new solution to the existing infrastructure of providing malware, worm or cyber-attack (protection) for SCADA system. Our research uniquely defines the following methods applied to provide a unique solution-

A. Malware Scanner
B. VPN (Virtual Private Network)
C. Snort Rule

A. Malware Scanner:

Malware stands for malicious software. SCADA system is IoT based system so it is affected by these harmful software. Example - Stuxnet affect the PLC of Siemens due to which the Stuxnet nuclear power plant was affected a lot.



B. Snort Rule:

Snort rule helps to minimize the false positive alert, with its help we can avoid log from specific the particular IP and port with the help of this we avoid false positive alert log.

log !192.168.169.0/24 any-> 192.168.169.0/24 111 (content:"|00 01 86 a5 | " msg "external mountd access":)

The major problem in a SCADA system is false negative logs. So, with snort rule all irrelevant logs will be removed and thus ultimately preventing DDOS attack via block particular IP.

C. *Virtual Private Network (VPN):*

VPN is used to protect your IP address. SCADA system is an IP based system so protection of IP address is important. VPN helps to hide it in cyber world so that it prevents DDOS (distributed denial of service attack) and help to prevent brute forcing on login portal.

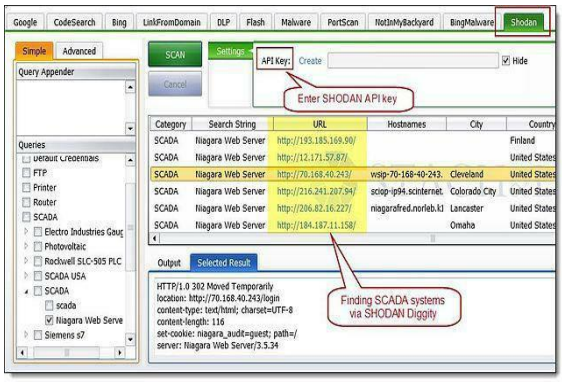
Because of search engines like Shodan anyone can figure out your SCADA system and it may be dangerous. So, VPN will help to solve this.

C.1 *How to configure Snort:*

We configure snort in SCADA OS with Wireshark and other tools like tcp dump. Snort is used to give an alert of particular IP and port through with suspicious connection which is trying to connect.

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "external mountd access";)

According to this it will block any connection between 192.168.0.1 to 192.168.1.255. Thus, preventing dos and other useless logs created by these IP.



C.2 Basic Header Rule of Snort:

Alert – Rule action. Snort will generate an alert when the set condition is met.

any – Source IP. Snort will look at all sources.

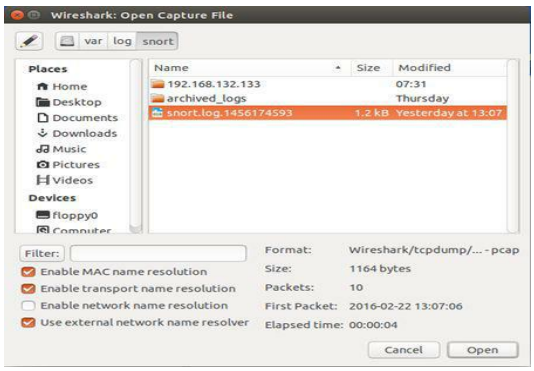
any – Source port. Snort will look at all ports.

-> – Direction. From source to destination.

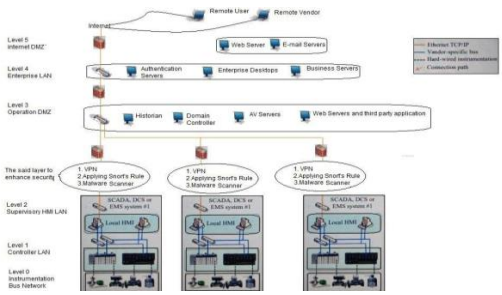
$HOME_NET – Destination IP. We are using the HOME_NET value from the snort.conf file.

any – Destination port. Snort will look at all ports on the protected network.

Via these we stop suspicious connection and Wireshark used to read the packet sent by the suspicious IP. So, all these steps help to remove all the useless logs and reduce chances of DoS.



(Way to capture the logs)



(The new architecture of SCADA system)

XIII.CONCLUSION:

The paper firmly presents an overview of the virtual data acquisition systems over the last 5 decades. It also explains the current system in place and the challenges facing it. The problem that needs to be addressed is to prevent attacks on the SCADA system because not only does it acquires data but also provides supervisory control over it. All the major industries use SCADA and hence are in constant danger of being hacked and therefore, a solution is required.

REFERENCES:

1. Alexandru UJVAROSI/EVOLUTION OF SCADA SYSTEMS/Bulletin of the Transilvania University of Braşov • Vol. 9 (58) No. 1 - 2016/Series I: Engineering Sciences
2. Russel, J.: A Brief History of SCADA/EMS/Available at: http://www.Scadahistory.com
3. Byres, E.: SCADA Security Basics: SCADA vs. ICS Terminology/Available at: https://www.tofinosecurity.com/blog/scada-security-basics-scadavs-ics-terminology
4. Zach Thornton/Virtual SCADA Systems for Cyber Security available at https://www.semanticscholar.org/paper/Virtual-SCADA-Systems-for-Cyber-Security-Thornton-Mudd/51ecfd13f8f8be6a3c31b8c75298e71667581033.
5. Development of the Intranet-based SCADA (supervisory control and data acquisition system) for power system/ Available at https://www.researchgate.net/publication/3850321_Development_of_the_Intranet-based_SCADA_supervisory_control_and_data_acquisition_system_for_power_system
6. DPD chronology/available at https://www.ibm.com/ibm/history/exhibits/dpd50/dpd50_chronology2.html
7. Data acquisition/ available at https://en.wikipedia.org/wiki/Data_acquisition
8. Nandini Raghavendra/scada systems/available at https://electricalfundablog.com/scada-system-components-architecture/
9. Alade A. A/Overview of the Supervisory Control and Data Acquisition (SCADA) System/International Journal of Scientific & Engineering Research Volume 8, Issue 10, October-2017 478 ISSN 2229-5518 /available at https://www.ijser.org/researchpaper/Overview-of-the-Supervisory-Control-and-Data-Acquisition-SCADA-System.pdf.

AUTHORS PROFILE

I, Ayush Chaturvedi is presently a 3rd year engineering student from Maharaja agrasen institute of technology. I was born and my initial studies was done in Varanasi , Uttar Pradesh. Being from an engineering background I always had a desire to explore new and emerging sectors and solve some challenging problems . Following the path of being an engineer I had an opportunity to work as an intern in some leading organizations in India such as Indian railways locomotive production unit , IIT bhu , election commission of India , glinks International. During those training period I came along one such cyber security problem in modern equipment handling software SCADA which I , with my friends tried to solve and after months of hard work we are pleased to share this paper with you all

I, Divyanshu Shekhar is a 3rd year undergrad student at Maharaja Agrasen Institute Of Technology. I am pursuing Bachelor Of Technology in Electrical and Electronics Engineering. I have been actively working on ways to improve the existing electrical systems using computer sciences. I believe that it is one of the best ways to enhance the efficiency of the system and also help in sustaining the environment.

I, Lakesh Goel was born and bought up in Panipat, Haryana. I am presently a 3rd year engineering student from Maharaja agrasen institute of technology. As far as I remember I've always been curious about how do people manage to operate several operations at a time from a command room. And my curiosity was further ignited when I finally had a chance to work at a thermal power plant, where I got to know about SCADA and the cyber problems concerning it. So after months of intense research my friends and I have come up with this paper.

I, Gaurav Sharma is a 3rd year undergraduate student at Maharaja Agrasen Institute Of Technology. I am pursuing my Bachelor Of Technology in Electrical and Electronics Engineering. I have been working on high end relays , which are so frequent in detecting faults in power grid. These relays should have very less frequency response time. It'll help to build a proper balance between consumer and power generation grid.

I, Harendra Kalyan is a 3rd year of B.Tech in EEE department from Maharaja Agrasen Institute of Technology. Being from a non-tech background it was initially challenging for me but at the same I had my curiousity levels spiked up as well. My interest towards Electrical department has risen only in my second year but as the saying goes "Better late than never", I've tried to increase my knowledge in this domain however possible eversince. I keep on learning more about this field through non-academic courses, training and my friends. My interests mainly lie in the merging of hardware and software components for easier and safer handling of technologies which are to come.