Novel Approach for Vulnerability Analysis in Pilot Smart Power Grid System

Dharmendra Yadav† and Dr. Anjali Mahajan††,
Govt. College of Eng. & Tech. Raj. India, Govt. Polytechnic, Nagpur, M.S., India

Abstract:
The term smart-grid was coined in early part of last decade and since then it has been developing rapidly across the wide range of energy generating and distributing systems such as solar energy, wind energy, bio fuels, geothermal and hydroelectric energy with an aim to improve the economy, safety and durability of power supply. On the down side, due to the distributed nature and complex architecture with multiple domain line like IT, power and telecommunication. There has been increase in dependency on cyber resources which may be vulnerable to attack. To tackle these issues a proper and efficient Information security risk management is required. In this paper, a novel framework for vulnerability analysis in smart power grid system has been presented which may be of tremendous potential and application for enhancing the cyber security of the smart grid. That is done through the case study of pilot grid in India with exposure evaluation existing well defined scoring system.

Keywords:
Smart-grid, Cyber security, Vulnerability, Reliability, Risk Analysis.

1. Introduction

Smart-grid is a two-way communication networks, where the grid operators and users of the system exchange information timely with the help of communication networks and control system [1].
Smart Grid is included in an ICS (Industrial Control Systems). SCADA of power grid has already been the part of ICS.
Therefore, to manage the various components of the generation, transmission, and distribution systems, current smart grid initiatives are focusing on expanding the use of ICT (Information Communication Technology) to modernize the current grid. However, this expanded use of ICT may lead to a greater number of attacks which could be as disastrous as a terrorist attack to key power plants or transmission lines
Emergence of Smart Grid, the increasing number of market participants, and the development of more complex market schemes make the physical system more vulnerable to cyber security risks. If attack against critical Smart-grid infrastructure is successful then it may result in a catastrophic impact to the entire power supply system, which may in turn adversely affect economy, and human safety.

Manuscript received July 5, 2016
Manuscript revised July 20, 2016

Security Vulnerabilities includes buffer overflow and protocol errors, denial of service that is degrading system availability. These systems often were not engineered to provide the robust levels of security needed to protect against an increasingly hostile cyberspace. In addition, there is a current trend to expand the connectivity of many critical infrastructure systems to provide improved control and monitoring capabilities.
As per The U.S. Department of Homeland Security (DHS) National Cyber Security Division's Control Systems Security Program (CSSP), ICS-CERT and the Cyber Security Evaluation Tool (CSET) [DHS] the common vulnerabilities are categorized as follows:
i)Weakness in ICS Software/ Product
ii) Weakness in Common ICS Configuration
iii) Weakness in Common ICS Network
As per the 2011 report of (DHS) top three vulnerabilities in ICS product assessment are improper input validation by ICS code, credential management and security configuration and Authentication weakness.
The top weakness found on the basis on incidence is like improper user permission and access control, weak password, patch management, lack of network policy.
The vulnerability of the electric grid more a matter of cyber security. The chief and main goal of cyber security risk analysis is to establish and know vulnerabilities, weakness and threats and point out their effects and influence [2]. The end result of the risk analysis should be the selection of tools to implement security controls for the effective smart grid.
Hence there is an ardent need to develop a suitable approach for Vulnerability analysis, so as to timely safeguard the novel Smart Power Grid System, which have been attempted in this paper.

2. State of Art

In this section, a brief review of some of the vulnerability risks that actual electric power systems faced has been presented.
In [3] Chee-Wooi Ten and M. Govindarasu have presented an attack-tree-based methodology for impact analysis have been developed for evaluating system, scenario and leaf level vulnerabilities.

In [4] YijunYu and VirginiaN.L have proposed open RISA (Risk Assessment in Security Argumentation) method that used Vulnerability as starting point to identify the security risk .It is an vulnerability driven approach , but they used common weakness catalogues. Weaknesses are errors that can lead to vulnerabilities.

In [5] S.Myagmar,J.Adam and W.Yurcik have developed unified, logical approach of threat modelling for complex systems .known vulnerabilities and threats yield a threat model . Here primary focus is on threat because it is a threat driven model.

In [6] A.Arora, A.Nandkumar and R.Telang have studied that the disclosure of vulnerability is risky or not. Here analysis is done on the CVE (common exposure and vulnerability) database and other sources with various permutation combination of known and unknown vulnerabilities with patched and unpatched vulnerabilities to understand the attacker's behavior.

In [7] A.Hahn and M.Govindarasu have used vulnerability assessment framework which uses various scanning and cracking techniques. The authors have also reviewed the already implemented technologies based on structured security methodology NIST 800-115. They have used an open source and software fuzzing test.

NIST 800-82 gives the Risk Management Framework [8] to protect the ICS (Industrial Control System) , in which Risk Analysis is very important for the effective Risk Management and it is an integral part of ISMS(Information Security management System). ICT enabled ICS are important from the Criticality point of view.

To get the efficient use of ISMS, automated tools/any Novel approach should be used for the Risk Analysis.

Smart grid is decentralized with the integration of ICT (Information Communication Technology) with OT (Operational Technology). In this the priority of triad security categories Confidentiality, Integrity, Availability (C, I, A) of is based on domains (ICT+OT) of the smart grid. When dealing with OT, the priority order is Availability, Integrity and Confidentiality (A, I, C), while when focusing on general purpose ICT processes Like smart metering, confidentiality is at the top (C, I, A) [16].

The objective of attackers is to focus on the weak exposure area and same principle they follow in case of Smart grid. In a successful attack the vulnerability will be exploited by threat agent. As per NIST 800-82, the primary part of Risk analysis is to do impact analysis to categories the security [9].

Our study is focused on OT so priority should be on Availability, Integrity, Confidentiality (A,I,C) . It is not necessary that all vulnerable components get exploited but it is a very important and first step after the Impact analysis to find vulnerability.

As per [15] the quality of security Mechanism/ controls implementation vary by type and size of industry ,study shows that best security controls are implemented in Finance sector . In production and other sectors quality of implementation is average. It shows that the focus on security implementation in ICS is not aggressive.

After analyzing the relevant work in this area, it is proposed to analyze Vulnerability in Smart Power Grid System under the proposed framework as described in the next section.

3. Proposed Framework

The proposed framework developed on the guidelines of NIST 800-82 [7-8] for tackling the above problem is presented in this Figure 1.

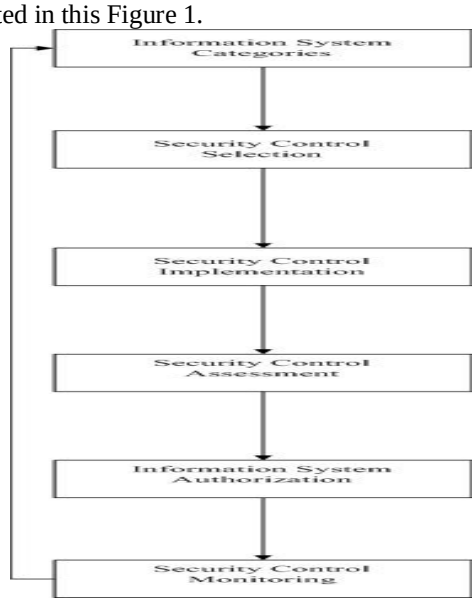

Figure 1: Risk Analysis Framework [9]

The composition and working of each block has been briefly described so as to have insight of working of the Risk Management framework of NIST800-82[9]:-

i. Information System Categories: On the basis of Impact analysis Information is to be processed, stored and transmitted .The information system is to be categorised, i.e. SC Security categories (Confidentiality, Integrity, Availability). The Risk analysis method is need to be decided.

ii. Security Control Selection: On the basis of security categorisation base line security controls are set for information system; Risk assessment is to be done considering the local condition .On the basis Risk assessment base line security control is to be supplemented with tailoring of controls.

iii. Security Control Implementation: Describe the working of controls with Information system and local environment, after successful implementation of controls.

iv. Security Control Assessment: The assessment of security controls using suitable assessment procedures to determine the level to which the controls are applied correctly, operating as proposed, and producing the desired outcome with respect to meeting the security requirements for the system.

v. Information System Authorization: Information system operation are authorized on the basis of determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the procedure of the information system and the decision that this risk is acceptable

vi. Security Control Monitoring: The security controls monitors the information system on continuous basis that comprising the assessing control effectiveness, documenting changes to the system or its environment of operation, the changes should be assessed through an Impact analysis, and the security state should be reported to the designated organizational officials

Approach that should be applied in implementing risk analysis is bottom-up techniques. It focuses on vulnerability and case analysis.

The scope of this paper is limited to vulnerability analysis which comes under Security Control Selection as a part of Risk analysis, hence the author will deal with this part in detail in the next section.

4. Methodology

The authors have studied one of the Smart Grid pilot project, which are running in India in different part of the 14 states.

The system configuration of the smart grid pilot project studied for the purpose of vulnerability analysis is under testing mode. The authors have developed Data Flow Diagram (DFD) for the data communication between data center, control center, substation and field.

On the basis of DFD with existing security mechanisms, the authors have developed exposure graph on the line of [7].The exposure path of the information objects have been evaluated and how attacker exploit the vulnerabilities. Related vulnerabilities issued by the ICS-CERT have been studied. For this, we considered the vulnerable components which get effected by the exposure graph and carried out vulnerability analysis for the system under study.To determine the effectiveness of the proposed approach, the feeder monitoring and control system of smart Grid (Pilot Project) was selected as a case study, as shown in Fig. 2

5. Case Study

Initially primary objective of Smart grid pilot project has been chosen as case study is to improve the following:[19].

i. AT&C loss due to power theft meter which is 36.1 %
ii. Absence of interconnection between feeder , due to which outage is there
iii. Accidental power outage
iv. Demand and supply gap is 17 %

In first phase, following things are planned [19]: -

i. AMI (Advanced metering Infrastructure) to automate the reading system from consumer to feeder to control system and also to avoid tampering of meter.
ii. PLM (Peak Load management) will work with AMI and SCADA (Supervisory Control And Data Acquisition)
iii. OM (Outage Management)
iv. Section and connection switch
v. S-SCADA is a Simplified –SCADA, well suited for necessary specially for the power distribution environment.

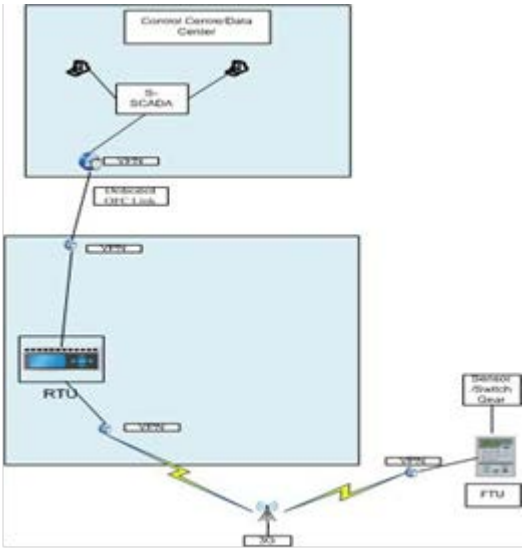

Figure 2: Feeder Monitoring and Control System of pilot project

Figure2 is the system configuration where Switching information of distribution section switches and distribution line measurement data obtained from sensors are sent via FTU (Field Terminal Unit) to the RTU (Remote Terminal Unit) of substation.

Substation RTU makes communications via S-SCADA using a DNP3.For communication between FTU and RTU of substation, 3G service is used .The SCADA-AMI can be connected via SOA (Service Oriented Architecture) in accordance with international standard with configuring a database in XML format conforming to IEC.

This system is considered for the analysis of security mechanisms, exposure evaluation and vulnerability. On the line of [7] privileges P with Security mechanisms and IO objects are identified. The DFD with security mechanism is drawn, shown in Figure 3, on the line of [17].

For this purpose, we have considered following Information Objects (IO) which is considered necessary.
1. Circuit Breaker (Datacenter→RTU→FTU→Sensor)
2. Read Status (Datacenter ←RTU←FTU←Sensor)
3. Read Voltage (Datacenter→ RTU-→ FTU-→Sensor)
4. Input-Output Status (RTU← FTU←Sensor)
5. Operation Status (RTU←FTU←Sensor)
6. Fault Detection Control(RTU→FTU→Sensor)

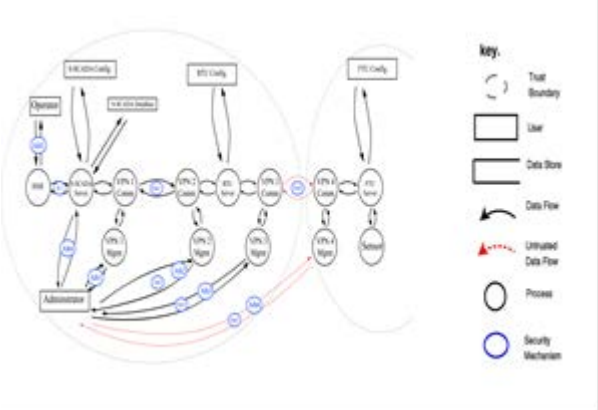

Figure 3: DFD with security mechanism of pilot project(feeder monitoring –control system)

In this as base line security policy is implemented considering that any attribute/data (Information Object) should be accessible through some privilege and security mechanism should protect that privilege. These security measures are compliant with NIST7628, U.S. standards.

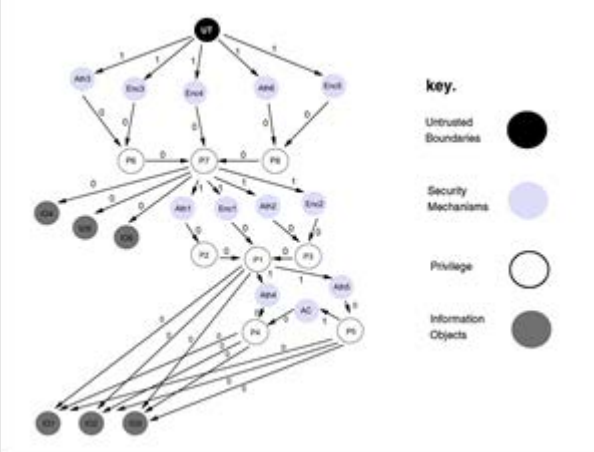

Figure 4 : Exposed graph

Massive data transmission should be prevented mainly with technologies such as “authentication”, VPN, Encryption and Access control. These are the security mechanisms, trusted perimeter should be defined. Security measures like anti-virus measures, fire-wall installation and IDS are used.

6. Result

Information model of (Control Center-Substation –Field Station) Pilot project is developed with proper security mechanism. Data flow diagram (DFD) which is then exploited to classify the trusted boundaries and type (trusted / untrusted) of data Input. Exposure algorithm [7] is evaluated and from untrusted network it identify attack surface and exposure of Information object is identified and here exposure for IO4, IO5,IO6 is 5 . The paths are {UT,Ath3,P6,P7,IO},{UT,Enc3.P6,P7,IO}{UT,Enc4.P7,IO} {UT,Ath6,P8,P7,IO},{UT,Enc5.P8,P7,IO}
It is presumed that once the attacker got the access. He will not explore other alternatives.
The Information Objects (IO4, IO5, and IO6) gets the link with vulnerable component /location (here it is RTU) through exposure path and untrusted entry point. The Information Objects /attributes which are exposed to attack surface are produce or consumed by the RTU. Table I gives detail of Exposed Vulnerable Asset (RTU) with score of Base value and Sub value of exploitability and vulnerability, which is calculated based on CVSS (Common Vulnerability Scoring System) [12]. The threat agent can exploit vulnerabilities. RTU has many vulnerabilities these can be exploited by different ways depend upon the Impact and Exploitability of vulnerability and exposure path.
The exposure path is evaluated by the algorithm of A.Hahn and M.Govindarasu [7] .Impact and exploitability is projected by the ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). ICS-CERT is maintaining record of exploits, vulnerability and any current issues. ICS-CERT advisories, NISTs NVD (National Vulnerability Database) gives the score of each vulnerabilities, based on CVSS [13, 14]. The vulnerability of RTU is taken from the ICS-CERT. The level of risk is pretended by the vulnerability scoring system, it will be helpful to prioritize the reaction.
As shown in Table I three vulnerabilities are of different types but there Exploitability sub score is 10 ,.its highly critical and there exploitability vector is same . In case of Impact sub score it is 2.9. Here impact vector, confidentiality is partial, in vulnerabilities CVE-2015-6485 and CVE-2016-2282. In vulnerabilityCVE-2013-6143the impact vector Availability is Partial. The asset, RTU is a part of OT, so Availability is of higher priority. The risk mitigation and implementation of Security mechanism is to be decided after detailed evaluation of CVSS vector.
Impact metrics is used for Confidentiality Impact, Integrity Impact, and Availability Impact. Exploitability metrics used for Attack Vector (AV), Access Complexity (AC), and Authentication (AU) [12].

TABLE I. Detail of Exposed Vulnerable Asset and Score based on CVSS

ASSET	VULNERABILITY	DESCRIPTION	CVSS B. SCORE	VECTOR	IMPACT SUB.SCORE	EXPLOITABILITY SUB SCORE
RTU	Improper Input Validation (CVE-2013-6143)	Through malformed DNP 3 traffic allows invalid input. As a result gives Denial of Service (temporary)	5.0	(AV:N/AC:L/Au:N/C:N/I:N/A:P)	2.9	10
RTU	Improper Ethernet Frame padding (CVE-2015-6485)	Before implementation of firmware its allow the attacker to get sensitive information of padding field of Ethernet	5.0	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	2.9	10
RTU	Directory Traversal (CVE-2015-3939)	An internal service interface of communication gives access through telnet. Exposed files contains the passwords to access interface.	6.8	(AV:N/AC:L/Au:S/C:C/I:N/A:N)	6.9	8
RTU	Insufficiently Protected Credential (CVE-2016-2282)	The authentication credentials are not protected properly means it's not encrypted properly	5.0	(AV:N/AC:L/Au:N/C:P/I:N/A:N)	2.9	10

7. Conclusion

Exposure metrics is a good evaluation frame work to enhance the risk management frame work of NIST 800—82 Major issue is once the exposure path is found. What methodology is used to select the security mechanisms /controls to mitigate the risk?

As per [7] once new security mechanism is developed again exposure evaluation is to be done .It has pragmatic difficulty in a distributed and large environment like smart grid.

Earlier there was belief that information security is a technical issue and it was logical because most of the asset require protection are of technical in nature. As the Security system is maturing at enterprise level. From many study, it can be concluded that security problems can't be solved alone on the basis of technology because information Security isn't purely a technical problem. It's also a social and organizational problem [11].

In this case study let's consider practical scenario where 3G is used for the communication between RTU and FTU as shown in Fig.2. VPN is used with proper security mechanism. In this scenario if any FTU is down for maintenance work .Operator uses this 3G for personal browsing and if it browsed unwanted website download malicious software etc. The probability of exploiting any zero day vulnerabilities will be very high.

8. Discussion

Practically in cyber security, risk is usually associated with some harm or loss to systems or data, Cyber security's approach to risk can reflect the relative immaturity of the industry and our responses to the professional challenges we face.

Maximum the problem is due the lack of systematic methodology for collecting and analysing historical data (vulnerability, attack and Incident) in maximum sectors .It is very important for experience and learning point of view.

As per [15] Following domains of security Controls/Security mechanism are the worst Implemented:

i. Business continuity/incident response
ii. Help desk/IT support training
iii. Physical security
iv. Testing and review
v. Network auditing and logging
vi. Sensitive data handling and protection

The quality of implementation of security mechanism is very important. Normally it has been observed that in most of sectors security controls /mechanisms are implemented on the basis of present or not. There is no methodology adopted in most of the sectors to analyse the quality of security mechanisms/controls implemented.

Proper security metrics should be there to understand the social, cultural and organizational, aspects of any organisation

The chances of vulnerability in Smart grid will be high. To protect this a Risk management frame work NIST 800-82 and NIST 7628 should be followed. Proposed framework should focus on the Vulnerability analysis considering the more serious zero day vulnerability and it should be mitigated with proper combination of all three security controls defined by NIST[18] . The more focus will be on worst implemented domain as mentioned above. The approach should be dynamic as well as adaptive in nature.

Acknowledgment

The authors would like to thank Mr. Himanshu Sheokand in charge of Smart Grid pilot project Panipat.

References

[1] U.S. Department of Energy, [Online] Available: www.oe.energy.gov
[2] A.Giani, E.Bitar, M.McQueen, P. Khargonekar, K. Poolla, M. Garcia, Smart grid data integrity attacks: Characterizations and countermeasures, in: Proc. of IEEE Conference on Smart Grid Communications, 2011
[3] C.-W. Ten, M. Govindarasu," Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 4, pp. 853–865, Jul. 2010
[4] N.LVirginia, T. T. Tun, Y.Yijun, R. Wieringa, B. Nuseibeh, "Risk and Argument: A Risk-based Argumentation Method for Practical Security," in ProcIEEE 19th International Requirements Engineering Conference. , pp. 239-248, 2011
[5] S. Myagmar, A. Lee and W. Yurcik, "Threat modeling as a basis for security requirements", Proc. 2005 ACM

Workshop on Storage Security and Survivability (StorageSS\'05), pp. 94-102, 2005
[6] A.Arora, A.Nandkumar, R.Telang, "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis, "Inf Syst Front ,vol 8, n 5, pp. 350-368, Dec 2006
[7] A.Hahn, M.Govindarasu,"Cyber Attack Exposure Evaluation Framework for the Smart Grid" IEEE Trans. Smart Grid,vol. 2, pp. 835-843, Dec. 2011.
[8] Common Cybersecurity Vulnerabilities in Industrial Control Systems, [Online] Available: https://ics-cert.us-cert.gov
[9] K. Stouffer, J. Falco, and K. Scarfone, "NIST SP 800-82: Guide to Industrial Control Systems (ICS) security," National Institute of Standards and Technology, Tech. Rep., Sep. 2008
[10] Guidelines for Smart Grid Cyber Security, NISTIR 7628, National Institute for Standards and Technology, Aug. 2010
[11] G. Dhillon and J. Backhouse, "Information Systems Security Management in the New Millennium," Comm.ACM, vol. 43, no. 7, pp. 125–128,2000
[12] A Complete Guide to the Common Vulnerability Scoring System Version 2.0, [Online] https://www.first.org/cvss/v2/guide
[13] NVD Vulnerability Summary [Online] Available:https://nvd.nist.gov
[14] ICS-CERT Advisories [Online] Available:https://ics-cert.us-cert.gov/advisories
[15] H. W. Baker and L.Wallace, "Is Security information Security Under Control ?," IEEE Security& Privacy, vol. 5, no. 1, 2007, pp. 35-44.
[16] EEgozcue,D.H.Rodríguez,J.A.Ortiz,V.F.Villar,L.Tarrafeta,(2012),Recommendations for Europe and Member States [Online]
Available ,https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations[micro]
[17] F. Swiderski and W. Snyder, Threat Modeling. Redmond, WA: Microsoft Press, 2004
[18] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems,"Nat'l Inst. of Standards and Technology, US Dept. of Commerce [Online] Available:http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[19] PilotProject[Online],Available:http://www.nedo.go.jp/library/seika/shosai_201408/20140000000607.html

Dharmendra Yadav received the B.E and M.Tech. degrees in Computer Technology and Computer Science respectively. He is pursuing PhD from G H Raisoni College of Engineering, research Centre under Nagpur University . He is IRCA ISO 27001:2013 Lead Auditor on Information Security from British Standards Institute. He is National EC Member of ISTE .He is currently an Assistant Professor in Computer Science and Engineering department at Govt. College of Engineering and Technology Bikaner, India.

Anjali R Mahajan, currently working as Head of Department, Govt. Polytechnic, Nagpur, completed her B.E. in Computer Science and Engineering from Government College of Engineering, Amravati in the year 1994, M.E in Computer Science and Engineering from Sant Gadge Baba Amravati University in the year 2002 and Ph.D. in Computer Science and Engineering from Sant Gadge Baba Amravati University. Dr. Mahajan has to her credit several publications in National, International Journals and National, International conferences. Dr. Mahajan is recognized guide for ME by research and Ph.D. in Computer Science and Engineering. Dr. Mahajan is Life Member of ISTE, CSI and member of IEEE