Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 777 – 781

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Cyber Physical Systems & Public Utility in India: State of Art

Santosh Kumar Majhi[a], Ganesh Patra[b,*], Sunil Kumar Dhal[c]

[a]*VSS University of Technology, Burla, India*
[b]*Utkal University, Bhubaneswar, India*
[c]*Sri Sri University, Cuttack, Odisha, India*

Abstract

The cyber physical system safety and security is one of the important and potential research directions recent days. Ongoing advances in science and engineering is going to improve the link between computational and physical elements by means of intelligent mechanisms, dramatically increasing the adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of cyber-physical systems. The transformation of physical systems into cyber-physical systems (CPS) by imbibing them with intelligence is an ongoing process that can substantially benefit the society and the environment by improving comfort, convenience and quality of life of the people, while reducing consumption of natural resources and reducing environmental footprint. Examples of cyber physical systems are Smart Grid Networks, Smart Transportation System, Enterprise Cloud Infrastructure, Utility Service Infrastructure for Smart Cities, etc. But, the inherent dangers in this transformation are: it allows flexible control and resource use; provides conduits for information leakage; prone to misconfigurations and deliberate attacks by outsiders and insiders. In this paper we discuss the state of art of cyber physical systems and smart utilities.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: cyber-physical systems; smart grid; cyber computing; enterprise cloud; smart city;

1. Introduction

A significant transformation is going on in efficient and automatic management of national physical system infrastructures[1 2 5] ranging from public utility service infrastructures, transportation to mobile health

* Corresponding author. Tel.: +91-8908757907
E-mail address:ganeshpatra099@gmail.com

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.052

management and telemedicine, disaster management. Cyber computing[10 11] is essentially being used to efficiently access, control and interact/communicate with such physical systems[2 6]. Cloud computing[3 4] and Internet-of-things technologies[7 9] are also being integrated with cyber computing space to manage and maintain large scale physical system infrastructures. Smart Grid Infrastructure[8 2] is one of such public utility service physical infrastructure which are largely deployed in United States. In coming 10 years, it will be deployed in large scale across all the major cities in India[12]. Recently, Govt of India has announced investment of Rs. 7060 crore in building 100 smart cities[13] where major transformation will be automating utility functions, building urban systems that can be monitored, analysed and improved upon to lead to better efficiency, equity and quality of life for the citizens. In addition, intelligent systems will be developed to improve its environment, monitor energy usage, provide personalized health and human service, ensure full spectrum public safety and security with integrated transport system while conserving and treating water. Functional failure and security threats to such large scale physical infrastructure may cause physical infrastructure breakdown, service outage, damage to the national resource and loss of life. Information Technology Act 2000 & Amendment Act 2010[14 15] by Govt. of India designates CERT as the National Nodal agency to serve to perform the following functions in the area of cyber security: (i) Collection, analysis and dissemination of information on cyber incidents; (ii) Forecast and alerts of cyber security incidents; (iii) Emergency measures for handling cyber security incidents; (iv) Coordination of cyber incident response activities; (v) Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

2. Sate of Art

In this section, we present various security threats, incidents and related challenges on cyber physical systems. We limit our study to focused directions of our proposed research: (i) Enterprise Cloud; (ii) Smart Grid.

In India, cloud computing infrastructure is being deployed in e-governance, mobile and remote health monitoring, real-time diagnosis, and smart technologies. The mostly cited threats[16 17] in cloud computing environment include compromising physical resources (computing systems, storage devices, servers, etc.) while running critical operations; tampering of cloud resident data and computing resources[17], and denial-of-service attacks on cloud-resident data[17 18]. Most enterprises and cloud service providers in India are using several ad-hoc enforcement methods (not standardized) to secure the computing infrastructure and services: a private cloud with enterprise perimeters[19], public cloud with service gateways[20], content encryption[20], session containers[19], runtime security virtualization [20], etc.

In healthcare cloud, medical data/information (inclusive medical image and videos) can be accessed and processed remotely in unknown cyber components (servers, machines) and are transmitted through wireless communication and sensor networks. For example, in mobile health and remote diagnostics, patient health record are dynamically captured (using sensors, medical signal processing devices) and processed on the fly (real-time) through various medical devices and exposed to cyber computing systems (i.e., wireless sensors networks) for further processing and transmission. The lack of secured cyber computing environment in such scenario may potentially cause tampering of medical records that may lead to incorrect diagnosis[21] and delayed treatment[22] to loss of life. In addition it may cause security attacks on physical components[23] in the cloud infrastructure (network jamming, flooding, denial-of-service). Moreover, medical data can be exposed to the social network of the medical professionals. Govt of India has initiated various healthcare initiatives[24 25] (such as, quality medical and surgical care for catastrophic illness, preventive medication, telemedicine) through NIC (National Informatics Centre) and IHO (Indian health organization). In addition, initiative has been made for medical standards and practices in India with the help of 3M and NABH (National Accreditation Board for Hospitals)[26]. International Medical Informatics Association (IMIA) is set up to investigate the issues of data protection and security within the healthcare

environment. Its work to date has mainly concentrated on security in EHR networked systems and common security solutions for communicating medical data[27]. The European AIM/SEISMED (Advanced Informatics in Medicine/Secure Environment for Information Systems in Medicine) project is initiated to address a wide spectrum of security issues in mobile healthcare[28 29 30].

Smart Grid Infrastructure[2] is one of the most important public utility service networks which are largely deployed in US. In coming 10 years, smart grid will be also deployed in large scale across the major cities in India. The correct and secure functioning of AMI (Advanced metering infrastructure) networks stand on consistent and secure execution of sequence of tasks. The secure configuration depends not only on the local device parameters but also on the logical interaction of these configuration parameters across the system. AMI contains millions of configurations parameters that exhibit a significant number of logical constraints and interdependencies that must be satisfied in order to preserve secure and safe interaction between various AMI components. Security threats to such large scale Smart Grid infrastructure due to misconfiguration and violation of security controls can cause massive power outages and damages to the national resource. Recent studies[31 32 33 34 35] reveals that 60-80% of security vulnerabilities are manifested in the cyber-physical systems due to network misconfigurations and lack of appropriate security controls. December 2008 report[36] from Center for Strategic and International Studies "Securing Cyberspace for the 44th Presidency" states that "inappropriate or incorrect security configurations were responsible for 80% of Air Force vulnerabilities". Juniper Networks report[37] "What is Behind Network Downtime?" states that "human misconfigurations are responsible for **50 to 80 percent** of network device outages". AMI security threats due to misconfiguration and violation of security controls can be extremely devastating and can cause massive power outages and damages. Thus, it is evidently essential to evaluate the protection capabilities of smart grid AMI configuration against dormant security threats such as device blocking, data un-reachability, data loss, tampering of data and denial-of-service attacks. Thus, it is evidently essential to evaluate the protection capabilities of smart grid AMI configuration against dormant security threats such as device blocking, data un-reachability, data loss, tampering of data and denial-of-service attacks.

An effort has been made by DHS AMI Task Force[37], and NISTIR[33 34 38], to create more than 300 security controls guidelines and metrics for AMI. However, the manual analysis for checking compliance and enforcement of these controls can be overwhelming and potentially inaccurate due to human errors. Moreover, the dynamic data transfer that allows meters, collectors and head end systems to use pull- or push-driven data delivery and the complex interaction with cyber devices require creating new formal models and analytic techniques for AMI.ConfigChecker[39], MulVAL[40], FINSAT[41] tools are proposed for analyzing misconfiguration problems in traditional networks. AMI vulnerability testing[42 43 44] can test the AMI devices against specific set of vulnerabilities. Studies are made on various attacks such as, false data injection, targeted disconnect attack[33 35 37]. Anwar et. all describes modeling & simulation of power grid controls[45 46]. The major limitation of the existing works is that they rely on probabilistic analysis which not provable. In addition these work focus on specific attack/vulnerability but not general based on AMI configuration. Moreover the existing methods can be applicable for invasive test analysis of small-scale smart grid infrastructure.

Central Electricity Authority constituted five committee to enquire the grid disturbance in Northern, Eastern & North Eastern Region on 30th July, 2012[47 48]. These committee focused its examination on (i) status of IT intervention in the operation of power sector; (ii) measures taken by various stakeholders to counter any possible cyber attack in their system; (iii) communication facilities available between various stake holders; (iv) formulation and enactment of Cyber Security Policy for Indian Power Sector in synchronization with CERT Transmission /Thermal/Hydro; (v) Strengthening of Communication Network through laying of Optical Fiber cables by State Transmission & Distribution utilities.*(1)*

3. Conclusions

We present various security threats, incidents and related challenges on cyber physical systems. We broadly discuss the challenges and research directions for Enterprise cloud and smart grid utilities. This discussion will help to discuss various experimental set-up, test beds, and infrastructure support required for developing Cyber Security

mechanism. Furthermore, this discussion will enable to understand the new potential challenges and possible solutions to address those.

References

1. M. Iorga and Scott Shorter, “Advanced Metering Infrastructure Smart Meter Upgradability Test Framework”, NISTIR 7823 Report, July 2012, pp 1-67.

2. M. A. Faisal, Z. Aung, J. R. Williams and A. Sanchez, “Securing Advanced Metering Infrastructure using Intrusion Detection System with Data Stream Mining”, PAISI 2012, Springer Verlag,Kualalmpur, Malaysia, May 2012, pp. 96-111.

3. Olson, M., Chandy, K.M., “Performance Issues in Cloud Computing for Cyber-physical Applications ",IEEE International Conference on Cloud Computing (CLOUD),2011.

4. Ugale,B.A.Soni, P. ; Pema, T. ; Patil, A., " Role of cloud computing for smart grid of India and its cyber security", Nirma University International Conference on Engineering (NUiCONE),2011.

5. N. Botts and et.al, "Cloud Computing Architectures for the Underserved: Public Health Cyber infrastructures through a Network of HealthATMs," in the proceedings of 43rd Hawaii International Conference on System Sciences (HICSS), Hawaii, USA, Jan. 2010, pp.1-10

6. GunarSchirner, DenizErdogmus, Kaushik Chowdhury, TaskinPadir, "The Future of Human-in-the-Loop Cyber-Physical Systems," Computer, Jan. 2013, doi:10.1109/MC.2013.31, vol. 46, no. 1, pp. 36-45.

7. JayavardhanaGubbi,RajkumarBuyya,SlavenMarusic,MarimuthuPalaniswam, " Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions",Future Generation Comp. Syst. 29(7): 1645-1660 (2013).

8. Ye Yanet. al. " A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", Communications Surveys & Tutorials, IEEE, Volume 15, Issue1.

9. Bari, N. ; Mani, G. ; Berkovich, S., "Internet of Things as a Methodological Concept ", Fourth International Conference on Computing for Geospatial Research and Application (COM.Geo), 2013.

10. E. A. Lee, “Cyber-Physical Systems - Are ComputingFoundations Adequate?”NSF Workshop on Cyber-Physical Systems:Research Motivation, Techniques and Roadmap October 16 - 17, 2006.

11. Sheth, A. ; Anantharam, P. ; Henson, C., " Physical-Cyber-Social Computing: An Early 21st Century Approach “, IEEE Inteligent Systems, Volume 28, Issue 1.

12. Rihan, M., Ahmad, Mukhtar ; Salim Beg, M., "Developing smart grid in India: Background and progress ", IEEE PES Conference on Innovative Smart Grid Technologies - Middle East (ISGT Middle East), 2011.

13. Government to set up 100 smart cities, Times of India, timesofindia.indiatimes.com/india/Government-to-set-up-100-smart-cities/articleshow/38919516.cms, 23 July 2014.

14. The information technology act, 2000, ministry of law, justice and company affairs, Govt. of India, New Delhi, the 9th June, 2000

15. The information technology Amendment Act, ministry of law, justice and company affairs, Govt. of India, New Delhi, http://deity.gov.in/content/notifications

16. F.B. Shaikh and S. Haider, “Security Threats in Cloud Computing”, International Conference on Internet Technology and Secured Transactions, IEEE, Dec 2011, pp. 214-219.

17. E. Amoroso, " Practical Methods for Securing the Cloud," IEEE cloud computing, May, 2014, pp. 28-38

18. H. S. Bedi, S. Shiva, "Securing cloud infrastructure against co-resident DoS attacks using game theoretic defense mechanisms", Proceeding ICACCI '12 Proceedings of the International Conference on Advances in Computing, Communications and Informatics Pages 463-469.

19. E. Amoroso, “From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud,” IEEE Security and Privacy, vol. 11, no. 1, 2013, pp. 23–31.

20. S. Luo, Z. Lin, X. Chen, Z. Yang, J. Chen, " Virtualization security for cloud computing service”, International Conference on Cloud and Service Computing (CSC), 2011.

21. Lincoln D. Stein, " The Electronic Medical Record: Promises and Threats", Web Journal, Volume 2, Issue 3

22. Shih-Chih Chen, Shih-Chi Liu, Shing-Han Li, David C. Yen, " Understanding the Mediating Effects of Relationship Quality on Technology Acceptance: An Empirical Study of E-Appointment System ", Journal of Medical Systems, 2013

23. TurgutAslan, "Cloud physical security considerations", IBM Cloud Services and Products, February 22, 2012

24. "Annual Report to People on Health",Government of India Ministry of Health and Family Welfare December 2011.

25. Sharma Kalpa, " Health IT in Indian Healthcare System: A New Initiative", Research Journal of Recent Sciences, Vol. 1(6), 83-86, June (2012).

26. Up-gradation of standards & practices in healthcare in India (A 3M NABH joint initiative) – NABH, eIndia Health Submit 2013.

27. Wimalasiri, J.S. et. al., " Security of electronic health records based on Web services ", HEALTHCOM 2005.

28. R. Zhang, L. Lui, " Security Models and Requirements for Healthcare Application Clouds ",IEEE International Conference on Cloud Computing, CLOUD 2010, Miami, FL, USA, 5-10 July, 2010.

29. Assad Abbas, Samee. U. Khan , "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds", IEEE Journal of Biomedical and Health Informatics 01/2014.

30. Milan Vukićević, SandroRadovanović, MilošMilovanović, MiroslavMinović, “Cloud Based Metalearning System for Predictive Modeling of

Biomedical Data",The Scientific World Journal 04/2014.

31. M. AshiqurRahaman, E. Al-Shaer and P. Bera, A Noninvasive Threat Analyzer for Advanced Metering Infrastructure in Smart Grid", IEEE Trans. Of Smart Grid, 2013, vol 4(1), pp. 273-287.

32. E. Al-Shaer, W. Marrero, A. El-atawy, and K. Elbadawi. Network configuration in a box: Towards end-to- end verification of network reachability and security. In Proceedings of IEEE International Conference in Network Protocols (ICNP), New Jersey, USA, October 2009.

33. NISTIR 7628: Guidelines for smart grid cyber security. Smart Grid Interoperability Panel- Cyber Security Working Group, March 2010.

34. P. McDaniel and S. W. Smith, "Security and privacy challenges in smart grid," in Proc. IEEE Security Privacy, 2009, pp. 75–77.

35. Y.Wang, D. Ruan, J. Xu,M.Wen, and L. Deng, "Computational intelligence algorithms analysis for smart grid cyber security," in Lecture Notes in Computer Science. New York: Springer, 2010, vol. 6146, pp. 77–84.

36. Securing Cyberspace for the 44th Presidency, Centre for Strategic and International Studies Washington, DC, December 2008.

37. Juniper, "What is behind network downtime?" 2008.

38. M. Iorga and Scott Shorter, "Advanced Metering Infrastructure Smart Meter Upgradability Test Framework", NISTIR 7823 Report, July 2012, pp 1-67.

39. X. Ou, S. Govindavajhala, and A. Appel, "MulVAL: A logic-based network security analyzer," in Proc. USENIX Security Symp., pp. 113–128, 2005.

40. E. Al-shaer, W. Marrero, A. El-Atawy, and K. Elbadawi, "Network configuration in a box: Towards end-to-end verification of network reachability and security," in Proc. ICNP, 2009, pp. 107–116.

41. SoumyaMaity, PadmalochanBera, S. K. Ghosh, Ehab Al-Shaer, FINSAT: Formal Query based Network Security Configuration Analysis, IET Networks 2014.

42. P. McDaniel and S. W. Smith, "Security and privacy challenges in smart grid," in Proc. IEEE Security Privacy, 2009, pp. 75–77.

43. Security in the Smart Grid. Cary, North Carolina: ABB Inc., ABB White Paper,2009.

44. A. Greenberg, Congress Alarmed at Cyber-Vulnerability of Power Grid [Online]. Available:http://www.forbes.com/2008/05/22/cyberwarbreach-government-tech-security_cx_ag_0521cyber.html 2008

45. S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in Proc. Int. Workshop Critical Information Infrastructure Security, 2009, pp. 176–187.

46. Z. Anwar and R. H. Campbell, "Automated assessment of critical infrastructures for compliance to (CIP) best practice," in Proc. Int. Conf.Critical Infrastructure Protection, 2008, pp. 366–375.

47. Report of the enquiry committee on grid disturbance in northern region on 30th July 2012, http://cea.nic.in/reports/articles/god/grid_disturbance_report.pdf

48. Annual Report 2012-2013, Govt. of India, Ministry of Power, Central Electricity Authority , July 2013, http://cea.nic.in/reports/yearly/annual_rep/2012-13/ar_12_13.pdf.