Cyber Security Threats-Smart Grid Infrastructure

[1]SHANKAR KUMAR DAS, [2]SWAYAM SAMPURNA S NANDINI GIRI
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
Bhubaneswar Institute of Technology, Bhubaneswar, Odisha, India

ABSTRACT:
Smartgridisanevolvingnewpowersystemframework with ICT driven power equipment massively layeredstructure.Thenewgenerationsensors,smartmetersandelectronicdevicesareintegralcomponentsofsmartgrid.However, the upcoming deployment of smart devices at differentlayersfollowedbytheirintegrationwithcommunicationnetworks may introduce cyber threats. The interdependencies ofvarious subsystems functioning in the smart grid, if affected bycyber-attack,maybe vulnerable and greatly reduceefficiencyand reliability due to any one of the device not responding in realtime frame. The cyber security vulnerabilities become even moreevident due to the existing superannuated cyber infrastructure.This paper presents a critical review on expected cyber securitythreats in complex environment and addresses the grave concernof a secure cyber infrastructure and related developments. Anextensivereviewonthecybersecurityobjectivesandrequirementsalongwiththeriskevaluation processhasbeenundertaken.Thepaperanalysesconfidentialityandprivacyissues of entire components of smart power system. A criticalevaluationonupcomingchallengeswithinnovativeresearchconcernsishighlightedtoachievea roadmapofanimmunesmart grid infrastructure. This will further facilitate R&D andassociateddevelopments.

Keywords—yberinfrastructure,prosumer,PeakLoadManagement(PLM),DemandResponse(DR),ICT,WANs,SCADA,denial-of-service(DoS),cyber security,cyber-attack.

INTRODUCTION

Smartgridcanberegardedas"systemofsystems"thatwill expand its current capabilities of generation, transmissionand distribution to distributed generation, renewable energysources and electric vehicles. Smart grid delivers electricitybetween suppliers and prosumers using two way informationandcommunicationtechnology(ICT)andexchangingnearrealtimeinformationaboutthegridstatestoenablecontrolandautomationofintelligentdevices.Thisallowstheprosumertosaveenergyandreduceelectricitybillswhileincreasing reliability, efficiency, robustness and transparencyofthesystem.Itisenabledbynumeroustechnologicaladvances in sensing, measurement and control devices. Fig. 1showsthereferenceNISTmodelforthesmartgrid[19].Unlikethelegacypowersystems,thesmartgridprovidesbetter situational awareness regarding the state of the system[4]. Consequently, peak load management (PLM) and demandresponse(DR)canbeimplementedinordertoflattenthepeak demand. The smart grid also performs predictive analysis inorder to keep the power balanced. Likewise, the fusion of newstoragetechnologieswillsupplementinintelligentdemandprediction.

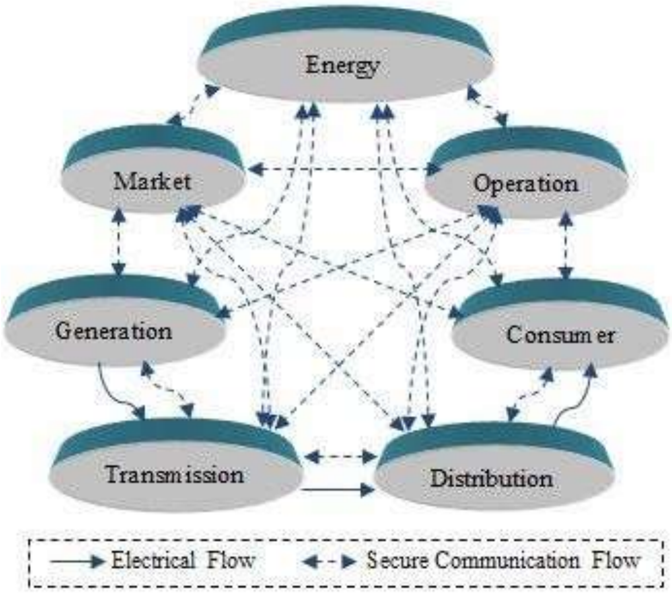

Fig.1.NISTreferencemodelforthesmartgrid

Thesmartgridisvisualizedtohomogenizehighspeedandtwo way communication technology with various power andcontrolequipment.However,suchasubstantialdependenceon information and communication networking increases therisk of potential vulnerabilities in the smart grid.This greatlyreduces the efficiency andreliabilityofthe power system,which, nonetheless, is the ultimate goal. Metkeet al. [25] haveshown that network infiltration by adversaries may lead toseriousconsequencesinthesmartgrid.AccordingtotheElectric Power Research Institute (EPRI) report, one of theupcoming challenges that the existing smart grid will face istheincreasingpossibilityofcyber-attacksandincidentsasincreasing number of devices are getting interconnected [5].Cyber security gets even more challenging when the scale andcomplexityofthesmartgridincreases. Variousresearchersandstandardbodieshavedevelopedcomprehensiveframeworks to tackle cyber threats and provide architecturalandanalyticalcountermeasurestopreventsuchattacks[16, 25]. Vulnerability assessment of electric power utilities alsoaidsinfindingthedesiredsolution[26].Itishowever,necessary to analyze and quantify the gravity of impacts ofcyber-attacks before any evaluation. This requires identifyingweak links within the cyber infrastructure. The grounds forcyber-attack on smart grid may range from economic reasons,pranks,disgruntledemployees,industrial espionage,andallthe way to terrorism.A feeble cyber infrastructure allows anadversary to infiltrate security through the weak links and thengain access to control software, and alter billing informationand load conditions to destabilize the system causing a majoreconomic disturbance. Furthermore, an adversary may invadeconsumers' privacy by collecting personal information. Thewide scale of smart grid makes it nearly impossible to provideimmunity to each and every component of such a complexnetwork.Tomakethesituationevenworse,sophisticatedcontrol architecture, state estimation and algorithms manifoldstheriskofattacks.ControlsystemmalwarelikeStuxnet,targeting vulnerable SCADA systems forced the utilities torethinkabouttheirexistingpowergridsecurity[2].Theutilities,thereforemusttakedecisionsonthechoiceoftechnicalsolutionswhencommissioninganewSCADAsystem or protecting an existing one. Cyber security must alsoaddressunintentionalcompromisesoftheinformationinfrastructureduetousererrors,equipmentfailures,andnaturaldisasters[16].ThecontemporaryITsecuritytechniquessuchasvirtualprivatenetworks(VPNs),publickey infrastructure (PKIs), intrusion detection systems (IDSs),firewall, anti-virus, etc.may be transplanted into the smartgrid, but due to their inherent differences they still cannot bemade effective without any enhancements [10]. The primarydifferenceisthetimecriticalnessofthenetworktrafficinsmart grid.The research on smart grid cyber security is ininfancy, this motivates us to thoroughly examine the systemcomponentsandidentifyallpossiblesecuritythreatsandexisting vulnerabilities in the smart grid cyber infrastructure.Thispaperfocusesonriskinspectionprocesswherecybersecurity assets are identified, checked for any vulnerability inthe system and later analyzed for the impact of the respectivecyber threats in the system operation. This will assist the smartgrid cyber security researchers in designing the appropriatecybersecurityarchitectureandnetworksystemstodeployappropriate countermeasures in order to prevent, detect andmitigate cyber-attacks in the smart grid. Section II, introducescybersecurityobjectivesandrequirementsinthesmartgrid.In Section III, risk assessment process along with analysis ofvarious security threats in the smart grid cyber infrastructureanditsassociatedimpactinsystemoperationhasbeenpresented, the need for data privacy and consumer protectionhas been highlighted in Section IV. Sections V concludes withfuturedirections.

I. CYBERSECURITYOBJECTIVESANDREQUIREMENTS

Thissectiondealswithcybersecurityobjectivesandrequirements in a smart grid cyber infrastructure. There arevarious organizations that have done extensive research on thedevelopments in cyber security objectives and requirementsincluding Electric Power Research Institute (EPRI), NationalInstituteofStandardsandTechnology(NIST),SmartGrid InteroperabilityPanel(SGiP)andIEEE.TheNISTreportexplainsthreehigh-levelcybersecurityobjectivesnamely:availability,integrityandconfidentiality.Apartfromsuchhigh-level security objectives for the smart grid, the NISTreportalsoaddressesspecificsecurityrequirementslikeidentification,authentication,authorization,trust,accesscontrolandprivacy[16].Theframeworksandguidelinesissued by such bodies needs to continuously evolve in order toensure a safe, scalable and reliable operation of the smart grid.The high-level security objectives for protecting the smart gridcyberinfrastructure aredescribedbelow.

- Confidentiality: Preventing unauthorized access by anadversary of highly secured information such as powerusage, price information and control commands thatintrudestheprivacyofcustomersandrevealstheproprietaryinformationofutilitiesiscalledconfidentiality.However,accordingtoKerckhoff'sprinciple [3], confidentiality of software should not betreated as important; rather focus should be given onthesecrecyofkeys.
- Integrity:Preventingmodificationofcriticalinformation of sensory devices, electronic equipment(e.g., smart meters), software and control commandwhichmightdisruptthe decisionmaking capabilityandcorrupt the data exchange of the smart gridiscalled integrity. Yi et al. [6] have shown that bad datainjection against the state estimation can compromisetheintegrityofthesmartgridcausingpowermismanagement.Unlikeincaseofconfidentiality,integrity of software should be kept critical because anadversarymightcontrolanydeviceorelectricalequipmentthroughcompromisedsoftware.
- Availability:Preventinganadversaryfromnotgranting access or control of the system to authorizedpersonneliscalledavailability.Denial-of-service(DoS) attacks and distributed DoS (DDoS) attacks candelay,blockorcorruptinformationcausingunavailability of power or information exchange in thesmartgrid.Inthiscase,availabilityofcontrolcommand and price information is critical as it cancauserevenueloss.

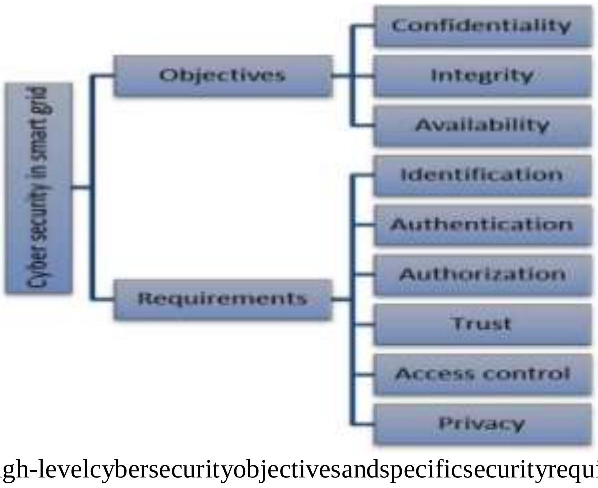

Fig.2.High-levelcybersecurityobjectivesandspecificsecurityrequirements

Fig. 2 shows the high-level cyber security objectives andspecificsecurityrequirements.Thespecificsecurityrequirementsareessentialforprotectionofcyberinfrastructureinordertoreduceliabilityandincreasecompetencyintheelectricmarketplace.Acomprehensiveanalysisofthespecificsecurityrequirementshavebeenundertaken inSectionIII&IV.

II. CYBER SECURITYTHREATS INSMARTGRIDItisexceedinglycrucialtocomprehendtheprospective vulnerability threats in the smart grid. In this section, the riskassessment methodology thatprovides a basis for exploitingthe possible entry points which are susceptible to maliciousattackshavebeenoutlined.Howtheseattacksallowanadversarytotakeunwantedactionsandconsequentlyaffecttheentiresmartgrid infrastructurehasalsobeenhighlighted.

A. RiskInspectionandAttenuation

Risk is the potential for an unwanted outcome resultingfrominternalorexternalfactors,asdeterminedfromthelikelihood of occurrence and the associated consequences [19].Simply risk may be defined as the union of likelihood of anattack, possible actions that an adversary may pursue and itsconsequentoutcomes.

Risk = Likelihood of Attack × Possible Actions × ConsequentOutcomes (1)

Thefirststepinriskinspectionisidentifyingthecybersecurity assets such as hardware devices, network parameters,softwareschemesandcommunicationprotocols.Thenmultiple testing schemes should be incorporated to check anyvulnerability in the existing power system. After the cybervulnerabilities have been identified, a comprehensive analysistodeterminetheimpactofanattackinboththeapplicationand physical layer of the smart grid infrastructure needs to becarriedout.Thisanalysiscanbedonebeperformedbysimulatingarealtimemodelandintentionallycreatingapseudo cyber-attack to observe the repercussions.Variousresearcheshavebeendoneunderthisdomaintoassistinanalyzing the possible threats and its impact to the supportinginfrastructure. Conte et al. [21] have studied vulnerabilities inthe smart grid using graph-theoretic approach while Kunduretal.[22] have modeledtheimpactofcyber-attacksthroughgraphbaseddynamicalsystems.Gianiatel.[20]haveanalyzed vulnerabilities and its impact to the legacy SCADAsystemsbydevelopingSCADAtestbedarchitecture.Theanalysisofprobablethreatsanditsimpacttothesystem environment have been identified; the next step is to find waystoalleviatetheprobableattacks. Desiredsecuritymeasuresandattackresistantsmartgridinfrastructureneedstobedeveloped and tested in real time environment. The results ofthetestshouldbeproperlyexaminedsoastoreducethepossibilityofanyfurthervulnerabilityandproposevalidmethods and protocols to mitigate such attacks. Also, guidancefrom security advisories and vendors; and knowledge fromalreadydeployedsecuritymeasuresneedtobeutilizedinorder to frame a resistant cyber infrastructure. An overview ofrisk evaluationprocessis shownin Fig.3.

B. ProbableAttackPointsandAdversaryAction

A smart grid cyber infrastructure is required to be modeledin such a manner that it is impervious to any invasion in thecyber workspace. This can be achieved only if the probableentry points which allow an adversary to invade the system isassessed. Legacy system which lack built-in security modulesin many devices and applications make the system vulnerable.Moreover, for a system with such large number of electricaland electronic connections along with mighty communicationchannels, it is very difficult tomake the entire smartgridcyber-attack resistant. But analyzing the different attack pointscouldhelpusplananddevelopsystemarchitecturesandprotocolswhichcanmakethesmartgridattackresistant.

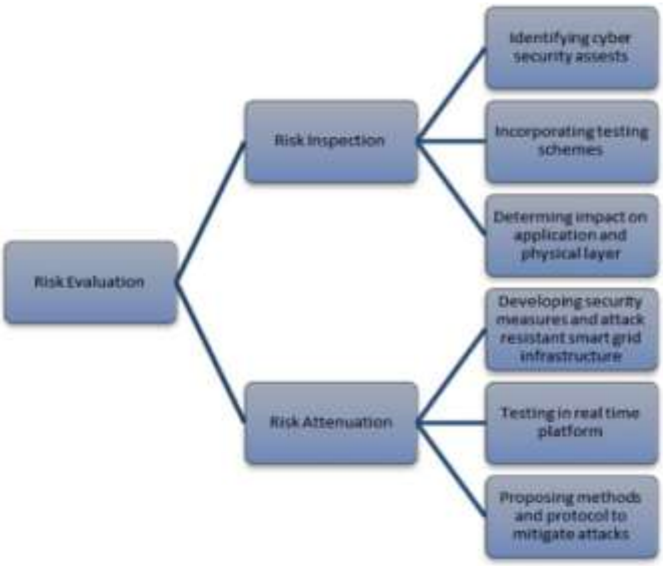

Fig.3.Riskevaluationprocess

Thevariousattackpointsinpowerindustrychainarelistedbelow:

1) GenerationSystem:

- The numerical relays in the generation plants adoptEthernet based IEC 61850 for information exchange.An adversary may launch a DoS attack causing therelay to mal operate during the fault conditions or mayevenaltertherelaysettingscausinginadvertenttrippingofrelays.Forexample,ifanattackersuccessfullydelaysthetr ansmissionofmessageincase of trip protection in generating stations then it cancauseseriousdamage tothepowerequipment.

- Variouslocal controlloops includingthatofspeedcontrol, valve control and AVR are linked with plantcontrolcenterthroughEthernet.Ifanadversarymanages to find security holes then it can easily gainaccess inside the local area network (LAN) and plant aTrojanorgetabackdoorentryhenceenablingtheadversary to compromise the digital control modulesbydisruptingthecontrollogic.Thiscouldbethehighestlevelofsecurity threat.

- The generation plants are monitored and controlled bytheSCADAsystem.LegacySCADAstilluseshardcodedpasswords,ladderlogicandlackauthentication. AnadversarymayeasilyinvadetheSCADAsystemtochange frequencymeasurementsprovidedtothe automatic governor control (AGC).Such an attack can directly affect the stability of thesystem.Mohajerinetal.[8]proposedatechniqueusing reachability analysis to measure the effect of anintrusionattack ontheAGC loop.
- RTUsandPLCsinpowerplantsgenerallyuseMODBUSorDNP3protocolsforcommunicationpurpose.The MODBUSprotocoldoesnotprovidesecurity against unauthorized entry. So an adversarywithIPconnectivitycancorruptRTUsorPLCsleadingtoundesiredsystemoperation.Similarly,DNP3protocolalsodoesnotemployencryption,authentication and authorization. So an attacker withnetworkaccesscaneasilyfabricatethemessages.Jinetal.[23]haveshownthat"bufferflooding"attackcanbeeasilydoneonaDNP3basedSCADAnetwork.Itisalsopossibletocreate"man-in-the-middle" attack [24] between the SCADA and the slavedevices (RTUs or PLCs) to get information regardingthenetwork topologyanddevice functionality.

2) TransmissionSystem:

- SCADA is the heart of transmission system at loaddispatch centers. It is now applied to larger and wideareanetworks(WANs)duetoadvancementininformationtechnology.Althoughloaddispatchcenters haveindependent control, but they arealsoconnectedtoothercentersthroughacommoncommunicationinfrastructure.Todaymanymajortransmission companies have integrated internet intothe communication network for better efficiency andreliability. But this puts the entire system at major riskbecause if an adversary manages to infiltrate any oneof the SCADA networks then it can cause havoc to theentire systemoperation.
- RTUs and PLCs also have the same vulnerabilities inthe transmission system as was in case of generationsystem. An adversary can specially craft an URL thatcanbesenttoanyoneatthecontrolcenter.AstheURLisopenedfromtheHMIconnectedtothenetwork, a malicious JavaScript snippet is executed inthe web browser [18]. This then automatically detectsthe PLCs connected to that network and invades thesystem.SuchattacksarecategorizedasCross-SiteRequestForgery (CSRF) attacks.
- Stateestimation,optimalpowerflowcomputation,economic dispatch and unit commitment studies aredone by algorithms embedded in software specificallydesigned to perform computations using thousands ofmeasurements. If an adversary manages to penetrateinsidethe networkandfalselyinject"baddata"or"redistribute load" then the system will immediatelyshift towards unstable operating conditions and impactthesmart grideconomicallyas well. Liuetal. [9]have createdfalse data injection attacks which manage topassthroughthesecurityduetobadidentificationalgorithms, provided they had the knowledge of thesystemconfiguration.ButYietal.[6]managestogoa step forward and inject stealth bad dataintothesystemwithlinearindependentcomponentanalysis(ICA) technique even without the knowledge of thenetwork topology.
- HVDC power lines are becoming paramount mode forbulkenergytransfer.Thepresentcybersecurityinfrastructure at HVDC links are substandard with noauthorization and access control features put into theirSCADAnetwork.Anadversarycansendcontrolsignals to change the commutation angle or may evenblock the power flow causing severe loss of power atthetargeted area.
- ModernFACTSdevicesuseshighspeedcommunicationlinktoexchangeinformationwitheachotherduring operation–henceincreasingthevulnerabilitiesinthesystem.AnattackercansendincorrectoperationaldatatotheFACTSdeviceresulting into unnecessary VAR compensation causinginstability.
- Integrationofrenewableenergyforecastswithrealtime system operations require advanced informationtechnology. Manipulation of wind and solar forecastdata sent to the control center can make the powersystemrunhaywireaffectingsystemoperationssuchas generation scheduling, dispatch, real time balancingand reserve requirements. Hackers might even go astepforward and reconfiguretheentire energygainand program the wind turbine to reverse its direction.Doing so, would not just harm the system operation,butalsodamage thewindfarms.

3) DistributionSystem:

- Aconventionalmetercanbemodifiedbyreversingthe internal usage counter or can be manipulated tocontrol the calculation of electric flow [12]. IntelligentElectronicDevices(IED)likesmartmeterscanbecontrolledtodeployvariousfunctionalitiesfromremote location. This enables an adversary to remotelyconnect or disconnect the devices or tamper with datasent to the system operator or sneak into confidentialdata of the consumers. Also, if an adversary managesto send false data packets to inject negative pricing inthe system then it will result in power shortages at thetargetedareacausinglossofrevenuetotheutilitycompany.Giventhattherearemillionsofconventional/smart meters connected to the system, itisdifficulttosecureeverynode–increasingthevulnerabilitiesofthesystemtomanifoldtimes.Anderson and Fuloria [11] have shown that an attackercouldswitch-offmillionsofsmartmeterssimultaneouslythrougharemotelocation.SmartmetersalsofailtocomplytotheOpenWebApplication Security Project (OWASP) standards suchas injection, authentication, cross site scripting (XSS),insecuredirectobjectreferences,security

misconfiguration,sensitivedataexposureandmissingfunction levelaccess control[17].

- NetworkingandcommunicationwithintheAMIinfrastructure will rely on technologies like WLAN,ZigBee, RF mesh, WiMax, WiFi and PLC. WirelessLocal Area Networks (WLANs) follow IEEE 802.11standardswhichbydefaultdonotprovideauthorizationmechanisms.Thisprotocolisalsovulnerable to traffic analysis [7], eavesdropping andsessionhijackingattacks.ZigBeeisbasedonIEEE 802.15.4 standards which are vulnerable to jammingattacks. Bennet and Wicker [13] have argued that theconventional ZigBee would suffer from delays due tomulti-tierfeatureofthecluster-treebasedroutingstrategy.Mobilecommunicationsaregenerallyunprotectedmediumsandcouldrevealenergyconsumptiondataandprovesusceptibletoprivacyinvasion. Worldwide Interoperability for MicrowaveAccess (WiMax) follows IEEE 802.16 standard whichare vulnerable to scrambling and replay attacks [7].Power Line Communication (PLC) can be susceptibleto threats by hostile users on the network using accesscontroltomisguideservices.NowadaysEthernetPassiveOpticalNetworks(EPON)isalsogettingpopularforelectricpowersystemdistributionautomation systems in smart grid [14]. But EPON toois vulnerable to attacks such as DoS, eavesdroppingandspoofing.
- An adversary can hijack the Virtual Private Network(VPN) of distribution utilities. The effects of slammerwormsmigratingthroughaVPNconnectiontoSCADAnetworkarereportedin[27].Thewormmanages to infect the control center LAN and blockedthe SCADA traffic. Such intrusions are particularlydangerous as they can be controlled and monitoredremotely.
- Due to lack of authentication and encryption at theHeadEndSystem(HES),anattackercandirectlytamper the Meter Data Management System (MDMS)and send unauthorized trip signals to the smart meters.Also,anadversarycanmasqueradesmartmetersconnectedat consumers'endandsend fakeenergyusage signals to the control center. Since the softwareinstalled at HES cannot spot the ambiguity, it executestherequiredcontrolandsendscommandtoturnoffthe smart meter. Such attacks can be very difficult totraceastheattackerimpersonatesasmartmeter.Kosutet al. [15] have shown that an adversary canattacktheEnergyManagementSystem(EMS)byfaking meter data. The firmware installed at the HEScan be also manipulated by changing the algorithmsdueto lackofproperaccess control.
- Consumers having net metering scheme installed attheirpremisescanalsofiddlewiththenetenergyusagedatasenttotheutility'scontrolcenterbyhacking into the communication network of the AMI.The attacker can reduce the electricity bill or may earncreditsintotheiraccounteveniftheconsumermight not be selling electricity to the grid. This directly doesnot affect the system operation but increases the lossesofdistributioncompanies.

4) TelemetryInfrastructure:

Telemetrysystemsareoftenneglectedduringsecurityplanning,testingandevaluationprocess.Theyconnectwith control systems and SCADA architecture of variouscomponentsinsmartgrid-generationsystems,transmission systems, distribution systems and micro grids.PowersystemtelemetryusesstandardcommunicationprotocolslikeModbus,IEC870-5-10x,DNP3andProfibus/Profinet. Irrespective of the type of protocol used,most ICS (Industrial Control System) protocols work on"master/slave" model having little or no security featuresand thus are susceptible to malicious network attacks. If anadversary gains access inside the "master" then the "slavedevices" can then be forced to spuriously operate or evenerase critical data. The above mentioned points highlightthetypeofattacksthatcanbemadeintothesystemwithout any physical presence of an adversary. However,there are certain ways in which system can be infiltrated byphysicalmeans.

- A disgruntled employee who has privilege to accessthe system components might alter the algorithms ofsoftware or may even change the settings of devicescausing spurious operation. Also corporate data can bestolen from the database for internal rivalry betweenthe competing service providers. Attacker can use keylogger software to gain access to system usernamesandpasswords.Suchactionsmightnotonlybedifficulttodetectbut also toprevent.

- Devices such as laptops and USB memory sticks thatare used both inside and outside the trusted perimetercangetinfectedwithmalwareoutside,andtheninvadethesystemwhenusedinside[4].
- Devices can also be compromised before deployingthemtothesitebychangingthesourcecodeofsoftwareortamperingwiththecontrolsettingsofhardware.Such attacksaresupplychain attacks[4].

III. DATAPRIVACYANDCONSUMERPROTECTIOND ataprivacyandconsumerprotectionremainstopconcern for the distribution utilities as well as consumers. Consumersneed to gain confidence to share their personal data to the thirdparty service providers or the utilities in order to improve theoperational efficiency of the smart grid. In this section, a briefoverview of the threats regarding privacy of the consumers hasbeengiven.Smartmetersinstalledattheconsumers'endexchange information with the home area network (HAN) orbuilding area network (BAN) regarding the data usage of theconsumersaswellassendcontrolsignalstothesmartappliancesinstalledattheconsumers'premises.Thesenetworkshowever,maybevulnerabletodataleakageoreavesdroppingthatcouldrevealactivitiesoftheconsumersand sensitive information like account numbers. For domesticconsumers, such data leakage could also reveal informationregardingthesmartappliances,plug-inelectricvehicles

(PEVs) and social networking activity which in turn exhibitsconsumers' personal behavior [1]. Also real time informationof energy usage may disclose whether a residence or facility isoccupied, wherepeopleare inthestructure,whataretheydoing,andsoon[16].Forindustrialandcommercialconsumers,suchdataleakagescanreveal highlysensitiveinformation for example the technologies used, manufacturingoutput, sale events, etc. This raises the prospect of industrialespionage amongst various competitors. On the otherhand,utilitiesandthirdpartyserviceprovideraggregateenergy usage data of different consumers for better demandforecast and peak load management. However, it is of growingconcern that such personal information can be comfortablyaccessed by any authorized personnel at the control center–making data privacy and consumer protection a strenuous jobforcyber securityresearchersanddevelopers.

CONCLUSIONS

Cyber security in smart grid is still under critical stage ofdevelopment.Thispaperpresentssmartgirdcyberinfrastructure framework within-depth research directions. Itisrequiredtoenhancetheconfidentiality,integrityandavailability of the system by building a robust and efficientsmart grid cyber infrastructure. Attack detection, mitigation,authentication and key management still remain challengingissues.Thecountermeasureschemeswithprotocolsforvulnerabilities need to be developed, tested and deployed. It isrecommendedtohavesecureprotocolbyregulatoryframework.

REFERENCES

[1] E. L. Quinn, "Smart metering and privacy: Existing laws and competingpolicies,"SSRN eLibrary,2009.

[2] J. Vijayan, "Stuxnetrenews power grid security concerns,"Computerworld,Jul.26,2010.

[3] A. Kerckhoffs, "La cryptographiemilitairie," J. Sciences Militaires, Vol.IX,pp.5–38,1883.

[4] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B.Sinopoli, "Cyber-physical security of a smart grid infrastructure," Proc.oftheIEEE,Vol.100,No.1,Jan.2012,pp.195-209.

[5] ElectricPowerResearchInstitute,"Reporttonistonsmartgridinteroperabilitystandardsroadmap,"2009.

[6] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li and L.Song,"Baddatainjectioninsmartgrid:attackanddefensemechanisms,"IEEECommunicationsMagazine,Jan.2013,pp.27-33.

[7] E.Bou-Harb,C.Fachkha,M.Pourzandi,M.Debbabi,andC.Assi,"Communication security for smart grid distribution networks," IEEECommunicationsMagazine,Jan.2013,pp.42-49.

[8] P.MohajerinEsfahani,M.Vrakopoulou,K.Margellos,J.Lygeros,andG.Andersson,"Cyberattackinatwo-areapowersystem:Impactidentification using reachability," Proc. Amer. Control Conf., Jul. 2010,pp.962–967.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks againststate estimation in electric power grids," Proc. 16th ACM Conf. Comput.Commun.Security,New York: ACM,2009,pp.21–32.

[10] J. Liu, Y. Xiao, S. Li, W. Lian and C. L. Philip Chen, "Cyber securityand privacy issues in smart grids," IEEE Communications Surveys &Tutorials,Vol.14,No.4,pp.981-997,FourthQuarter2012.

[11] R. Anderson and S. Fuloria, "Who controls the off switch?" Proc. 1stIEEESmartGridComm2010,Gaithersburg,MD,Oct.2010,pp.96-101.

[12] P. McDaniel and S. McLaughlin, "Security and privacy challenges in thesmart grid," IEEE Security and Privacy, Vol. 7, No. 3, May/Jun. 2009,pp.75-77.

[13] C.BennettandS.B.Wicker,"DecreasedtimedelayandsecurityenhancementrecommendationsforAMIsmartmeternetworks,"Innovative Smart Grid Technologies (ISGT 2010), Gaithersburg, MD,Jan.2010,pp.1-6.

[14] Z. Sun, S. Huo, Y. Ma, and F. Sun, "Security mechanism for smartdistributiongridusingethernetpassiveopticalnetwork,"2ndInternationalConferenceonAdvancedComputerControl(ICACC2010),

Vol.3,Shenyang,China,Mar.2010,pp.246-250.
[15] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks onsmartgridstateestimation:attackstrategiesandcountermeasures,"Proc. 1stIEEESmartGridComm2010, Gaithersburg, MD, Oct. 2010,pp.220-225.
[16] U.S.NIST,"Guidelinesforsmartgridcybersecurity(Vol.1to3),"NISTIR-7628,Aug.2010,
[17] Open Web Application Security Project, "Top 10 OWASP, 2013," Aug.21,2015
[18] Eduard Kovacs,"Flaws inrockwellPLCs expose operationalnetworks,"SecurityWeek,Oct.28,2015.
[19] U.S.NIST,"NISTframeworkandroadmapforsmartgridinteroperability standards, release 1.0," NIST Special Publication 1108,Jan.2010.
[20] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli and J. Wiley, "AtestbedforsecureandrobustSCADAsystems,"in:SIGBEDReview,Vol.5,No.2,ArticleNo.4,2008
[21] D. Conte de Leon, J. Alves-Foss, A. Krings and P. Oman, "Modelingcomplexcontrolsystemstoidentifyremotelyaccessibledevicesvulnerable to cyber attack," Proc.First Workshop on Scientific AspectsofCyberTerrorism, Washington DC,2002.
[22] D.Kundur,X.Feng,S.Liu,T.Zourntos,andK.L.Butler-Purry,"Towards a framework for cyber attack impact analysis of the electricsmart grid," Proc. IEEE Int. Conf. Smart Grid Commun., Oct. 2010, pp.244–249.
[23] D. Jin, D.M.Nicol, G. Yan, "An event buffer flooding attack in DNP3controlledSCADAsystems,"Proceedingsofthe2011WinterSimulationConference,2011.
[24] I.Fovino,A.Carcano,M.Masera,andA.Trombetta,"Designandimplementation of a secure Modbus protocol," Critical InfrastructureProtection III, Vol. 311, C. Palmer and S. Shenoi, Eds. Boston, MA:Springer-Verlag,2009,pp.83–96.
[25] A.R.Metke,R.L.Ekl,"Securitytechnologyforsmartgridnetworks,"IEEETransactionsonSmartGrid,No.1,June2010,pp.99–107.
[26] J. Yu, A. Mao, Z. Guo, "Vulnerability assessment of cyber security inpowerindustry,"Proc.ofIEEEPowerandEnergySocietyGeneralMeeting(PES '06),2006,pp.2200–2205.
[27] NorthAmericanElectricReliabilityCouncil,"SQLslammerwormlessonsleanredforconsiderationbytheelectricitysector,"Jun.2013.