JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Online Privacy and Cyber Security

Ankit Kumar, Ansh Pancholi, Shourya Kumawat, Sandeep Kumar Raj, Aman Raj

Vivekananda Global University, Jaipur, Rajasthan

Abstract:

With the advent of the digital age today, online privacy and cybersecurity have become a matter of serious concern for individuals, organizations, and governments alike. Due to the very rapid proliferation of the internet and its many connected devices, new opportunities for data collection, storage, and sharing have opened up. Still, such expansion also poses a serious threat to personal privacy and information security. Cybersecurity means the practices and technology built to defend systems, networks, and data from cyberattacks. In contrast, online privacy is more concerned with protecting personal data from unconsented access, misuse, and surveillance.

With these evolving online threats, the focus of organizations such as NASA has turned more poise on the protection of sensitive data from intrusion by cyber threats and the privacy of individuals interacting with their systems. As a result, NASA's cybersecurity not only reflects critical measures to protect their data, systems, and infrastructure but will also protect national security interests in the larger collective and promote trust in digital technologies. With sophisticated cyberattacks-including data breaches, ransomware, and phishing campaigns-NASA and other institutions must augment and perfect their cybersecurity measures so they can safeguard against these threats in an evolving fashion.

Various privacy regulations very few of them, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)-are on the rise owing to increasing concerns about restoring the ethical and legal consequences of collecting and surveilling data. But even the privacy laws, with good intentions, face paradoxes when balancing measures for both individual protection and counteracting threats to security. NASA's involvement in both stringent cyber protection and user privacy is critical not just to safeguard its missions and employees but lay the groundwork for other organizations that might be harboring private information.

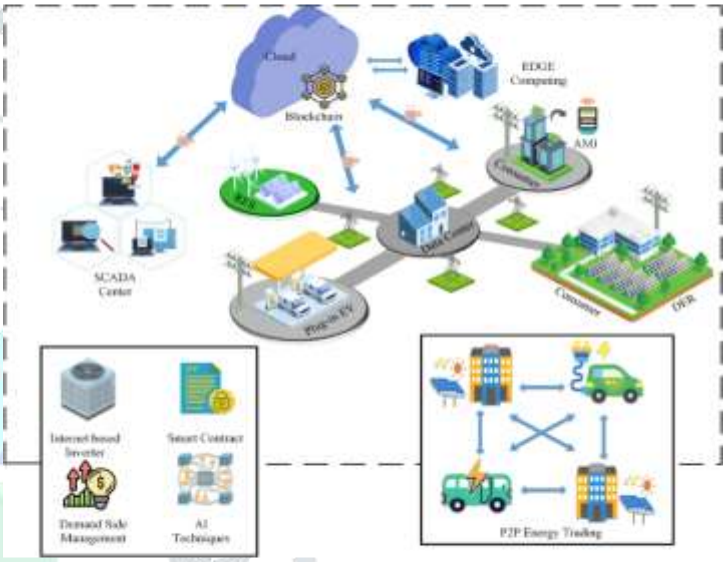
It will explore a crossroads where cyberspace privacy interfaces with cybersecurity and aims to present NASA's measures for dealing with such problems. The report delves into specific threats, privacy concerns, and cybersecurity measures to lessen risks. It also gives an overview of the ever-changing landscape of online privacy and cybersecurity and suggests recommendations to strengthen protections in light of emerging technologies and threats presented by an advanced technological system. In doing this, the report highlights the importance of striking a balance between the need to secure sensitive information and the need to observe individual privacy rights in an increasingly digital world.

Introduction:

The superhighway in the realm of electricity supply and distribution functions involves the incorporation of cyber security into power systems, owing to its advantages. It is therefore important to secure every data of communication or storage files that must remain confidential. Cyber security refers to the advanced digital infrastructure that is above the present electric grid. Another role of cyber security is monitoring the grid condition, energy consumption, generation, and distribution operations, and automation of the process. It is not merely a cable/data network that upgrades the existing electric grid with generation utilities, for longer transmission distances and end consumers consuming the electricity but also advances operations along the data network by isolating the fault and simplifying revenue collection. The goals, and aims of the smart grid are not limited, etc.

- Improve the reliability of the electrical grid
- Improve its overall efficiency
- Lower costs of distribution and generation
- Allow for real-time monitoring of the electrical grid

To accomplish this goal, the smart grid will use new microprocessor-based digital devices or instruments on both the customer and utility side. Smart meters are used to enable communication between the utility and customer side and provide them with data about the energy being consumed through an online monitoring system, grid conditions, and real-time data usage alerts to the end users.



1. CYBER VULNERABILITIES IN THE ECONOMIC POWER GRID:

The legacy power grid is managed by control equipment, protective devices, a real-time monitoring system at the substation end as well as the utility side and extensive communication network.

1.1 SCADA SECURITY:

SCADA is a traditional tool used for controlling and real-time monitoring of any existing system in the National power grid. It undergoes a cyber-attack assessment process in connection with the National SCADA Test Bed (NSTB) program. It is doing several tests or assessments of control system products, and onsite operational environment including facilities for electrical power grid facilities. Many vulnerabilities were found during the assessment, and these must then be classified and worked upon properly and expressed in the reports. A vulnerability should, therefore, be included as long as it is found in more than two assessments. Most of the SCADA vulnerabilities have yet to be disclosed in the public domain, as stated in NVB.

1.2 Substation Security:

A Private Company of Public-Private Partnership (PPP) must provide a close evaluation regarding the security of substation automation and its posture. The substation would have various devices ranging from distribution to transmission level devices, including capacitor banks, circuit breakers, phase-shifting transformers, relays, power transformers, isolators, and switching devices. The substation could also employ control and automation devices for controlling, measuring, and monitoring its various components. The level of automation and control on various devices is increasing, thus indirectly implying an increase in vulnerability levels against cyber security. Increased automation, does not, however, mean a compromise with security; however, the study positively identified several vulnerabilities of the automation devices within substations and then described the potential consequences of their exploitation. With the exploitation of the vulnerability, possible consequences would lead to cyber-attacks, directly affecting the destruction of generators, power outages, and grid instabilities.

1.3 Legacy Communication Network:

Various kinds of communication technology are employed in the power grid for operational support. Control Centers within utilities and regional transmission operators/independent system operators (RTOs/ISOs) are in constant communication with and among one another and with substations in the interests of balancing power generation and demand, maintaining voltages and frequencies, responding to changing conditions, maintaining real-time power market access, etc. The communication media used to exchange data between grid entities include frame relay networks, asynchronous transfer mode, the PSTN, the Internet, and wireless technologies such as wireless modems, microwaves, and satellites. There are many data exchange protocols used between entities or nodes within the power grid that overlap with those commonly employed in the Information Technology global domain, like TCP/IP, HTTP, and FTP. Protocols designed specifically for communication within control systems are, for example: DNP 3.0, which was specifically conceived for control system communication; also, the ICCP protocol was designed to enable grid control centers to communicate.

2. SECURITY OF CURRENT SMART GRID TECHNOLOGIES: Smart Meters, Advance Metering Infrastructure, and Automatic Meter Reading are in the category of Smart Grid. However, Smart grid technologies moreover known as Cyber Security Vulnerability.

2.1 AMI Security: Renewable energy integration fosters the development of another important sub-technology, namely, advanced metering infrastructure (AMI). It is the backbone technology giving rise to the making of smart grids from conventional power grids. It seems to be an enabling technology for smart grid technology from utility to end-user. AMI is so important that we must protect them very well from hackers, and e-threats with minimal vulnerable points. The AMI should be shielded from external threats that can cause large-scale damage to other systems, such as grid instability, etc.

2.2 Wireless Network Security: With the advent of Smart Grid concepts, wireless networks have found prominent deployments in the ecosystem. Wireless networks were adopted because they have certain outstanding advantages over the other alternatives. There are quite several wireless devices available on the market, which are low-cost. Some AMI implementations use wireless mesh networks to auto-route multi-path multi-hop communications between AMI nodes. Due to the multiple paths that could be taken between two random nodes for communicating, a mesh network can also be named a self-healing network. For example, ZigBee is a cheap, low-power, wireless mesh networking standard. The fact that it is cheap enables broad deployment, while low power consumption allows longer life with smaller batteries, and mesh networking provides high reliability along with a larger range. However, the mesh network is susceptible to being attacked by any intelligent adversary.

2.3 Potential Attack Scenario: Possibilities are, that if attackers were to gain access to the smart grid, they would probably issue false calls and messages to the utility side in the form of reducing demand from the end consumers. Such attacks will be carried out with sheer ease from the smart meters since their functionalities are based on microprocessor platforms and have a communication protocol, therefore making them susceptible to attacks. All this is a cause of Grid Instability, voltage fluctuations, and way too much confusion to set up a priority matrix for load shedding.

3. CYBER SECURITY ISSUES ON SMART GRID: Cyber-attacks have existed for as long as there have been computers. Cyber-attack protectors and the power operator of a power utility had to strongly equip the electric power utilities against the threats posed by the cyber world. The defense measures against these threats included an organization's strong internal information security programs; the government taking proactive measures to support US critical infrastructures; and communication protocols to protect against the various attack vectors. Stakeholder engagement aims to develop an operating environment whereby risky telecommunications systems can co-exist with electricity generation systems. Smart grid refers to a set of devices and communication systems focused on the cyber security of the power industry, taking into account the effect of all IT networks and communication problems on the distribution management and power delivery systems of utilities. It is in effect aimed at safeguarding the power grid from cyber disasters and unforeseen hazards, while preparing for, mitigating, and enabling recovery from such hazards. Grid security faces four sets of challenges that ought to be addressed. The new communication development in the power delivery sector requires a variety of protocols, latency, bandwidth, and operational costs. Adapting smart grid development requires positive action towards substitution or upgrading the other aspects. Many legacy devices used for communication and command processing have limited powers. It makes them more obsolete to different systems. Most act in very particular or limited manners, which causes a lag in operations, less memory space, and decreased computation.

3.1 Device Issue: Various devices are from the PLC, RTU, and IED family, which are functional in the modern power grid administration in performing several tasks and maintenance. Smart meters act like meters to calculate energy consumption; but, unlike conventional meters, they can communicate with the utility side! This means that smart meters can notify the consumer of how much energy is consumed every day, assisting the consumer in establishing their daily load pattern. Some of these would be under physical attacks, like battery removal/changing/some modification of meters or functions that remote connect/disconnect and outage reporting that could be exploited by third parties. The PHEV could be recharged at different locations, and inaccurate billing or unwarranted service will cast a plague on grid balance/stability.

3.2 Networking: "Internet" can be used anywhere which causes inherent threats like malicious malware files, and denial of services (DoS). "There are vulnerabilities to attacks on the wireless layer 2/3 layer. These happen from attacks of network protocol injection and modification. Until such operations are provided to the layer, routing does not perform as security traffic can't be considered reliable." "The sensor networks are so critical for the power grid that tampering, intercepting, and forging of the data will damage the grid security."

3.3 Dispatching and Management: "SCADA, EMS, DMS" distribution control commands and access logs for anyone leads severe for security and damages the grid operation. Synchronizing time-tagged data is essential in a wide area and without it can't be reliable for achieving the SCADA and their systems. Load management of EMS provides both active and passive control by both customers and service providers. Smart Grid consists of several technologies that are self-remarkable. Microgrid is one the best examples which is a decentralized distribution grid that works also on a Stand-alone system as well as with Tie Grid function. SCADA system is one of the major technologies which are used for monitoring "Islanding Operation" or "Islanding Mode". As per the framework, it ensures the reliability function of the smart grid. Here are some points considered the increasing risk of the system cannot be compromised.

1. Take Down the Server.
2. Gaining control over the system.
3. Stealing corporate data.
4. Fiddling with billing information.
5. Key logger software.
6. Gain competitive advantage.
7. Misuse the SCADA server.
8. Manipulate mathematical data points.
9. Change user-logged data in a distant and remote DBMS.

4. RECOMMENDATIONS FOR PRIVACY ISSUES: An NIST report on the privacy impact assessment (PIA) from the consumer to utility perspective on the smart grid was published. These principles of design to address privacy issues within the smart grid which is:

1. The organization should have appropriate security and privacy policies and practices and ensure they are documented and followed. Audit logs should be used to monitor all data access and modification.

2. A clear notice should be given before any notice is collected and shared about any personal data.

3. Options should be available to all users so that personal information is not disclosed.

4. Only the personal information necessary to accomplish the stated purpose will be collected from an individual.

5. FUTURE RESEARCH DIRECTION: Privacy-Preserving Technologies

Federated Learning: Creating techniques to allow AI model training on decentralized data without direct access to them.

Differential Privacy: Improving mechanisms to prevent individual data from being learned through queries to aggregate databases.

Encrypted Computation: Advancing homomorphic encryption and secure multi-party computation to the point where they can be used regularly to operate directly on encrypted data.

1. AI and Cybersecurity

AI-Driven Threat Detection: Machine learning is used to identify new and sophisticated attack patterns in real time.

Adversarial AI: Developing defenses against AI-enabled cyberattacks and adversarial examples that trick AI systems.

Explainable AI: Making AI-powered security systems more transparent to facilitate trust and accountability.

2. Internet of Things (IoT) Security: Lightweight Cryptography: To design security protocols that are suitable for resource-constrained IoT devices.

Firmware Security: Developing techniques to identify and remediate vulnerabilities in IoT firmware.

Autonomous Threat Mitigation: Developing self-healing IoT systems that can autonomously detect and respond to threats.

6. CONCLUSION: This paper gives an overview of cyber security and privacy issues in the smart grid. To existing To do that research, I might come to that nearly all IT-related things in a smart grid are technology. general IT environment, which needs to be more secure. This paper also provides the future directions for the research direction and we need to adopt new methodologies and techniques that are more secure than the ones already in place. Cyber Security and its privacy issues in smart grid are new areas in the field of power industry, electrical engineering, electronics technologies, and Computer science. More in-depth needs more research in the field of cyber security is required to. The fact that, if this goes well, we'll be able to develop such a promising power grid soon.

7. REFERENCES: [1] "Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues" by Wayne F. Boyer Scott A. McBride in April 2009.

[2] "Cyber Security and Privacy Issues in Smart Grids" by Jing Liu and Yang Xiao, Senior Member, IEEE, ShuhuiLi, Wei Liang, C. L. Philip Chen, Fellow IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 4, FOURTH QUARTER 2012.

[3] Cisco system Inc., "Internet protocol architecture for the smart grid", white paper, Jul. 2009, available at http;//www.cisco.com/web/strategy/docs/energy/CISC O_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf.

[4] U.S. DOE," Smart grid system report, "White paper, Jul. 2009, available at: http://www.oe.energy.gov/SRGMMain_090707_lowers. pdf "Cyber security in the smart grid", by India smart grid Knowledge portal available athttp://indiasmartgrid.org/en/technology/Pages/CyberSecurity.aspx.

[5] U.S. DOE, "Smart grid system report," White Paper, Jul.2009, available at: http://www.oe.energy.gov/SGSRMa in-090707 lowres.pdf.

[6] U.S. NETL, "A systems view of the modern grid," White Paper, Jan. 2007, available at: http://www.smartgrid.gov/white papers.

[7] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 1, Jan. 2009, pp. 16-26.

[8] D. Divan and H. Johal, “A smart grid for improving system reliability and asset utilization,” CES/IEEE 5th International Power Electronics and Motion Control Conference, Shanghai, China, Aug. 2006, pp. 1-7.