# Solutions and Suggestions for Smart Grid Threats and Vulnerabilities

Seref Sagiroglu*, Yavuz Canbay**‡, ilhami Colak***

* Department of Computer Engineering, Faculty of Engineering, Gazi University, Ankara, 06570, Turkey

** Department of Computer Engineering, Faculty of Engineering and Architecture, Sutcu Imam University, Kahramanmaras, 46050, Turkey

*** Faculty of Engineering and Architecture, Nisantasi University, Istanbul, 34398, Turkey

(ss@gazi.edu.tr, yavuzcanbay@ksu.edu.tr, ilhcol@gmail.com)

‡ Corresponding Author; Yavuz Canbay, Department of Computer Engineering, Faculty of Engineering and Architecture, Sutcu Imam University, Kahramanmaras, 46050, Turkey, Tel: +90 344 300 1705, yavuzcanbay@ksu.edu.tr

*Received: 26.04.2019 Accepted:28.12.2019*

**Abstract-** Smart grid systems are complex and huge power networks including many digital components and assets. These systems provide opportunities to operators to collect data remotely from customers and manage their network reliably and effectively. Therefore, the operators can track and analyze historical and immediate power consumption data, and take necessary actions to manage changes or meet the requirements of the consumers. Beside smart grid systems bring many advantages compared to traditional power systems, cyber security is one of the main challenging issues for these systems. In this paper, vulnerabilities and threats for smart grids were reviewed, categorized and evaluated for six components of smart grid systems, for the first time. Then cyber security considerations on smart grid systems were examined and discussed, and finally some applicable measures to minimize currently available vulnerabilities and threats were presented.

**Keywords** Smart grid, threat, vulnerability, cyber security, review.

## 1. Introduction

Smart grids are huge and complex networks including different types of connected assets. It enables power system operators to monitor, control, maintain and manage electrical systems, information and communication technologies (ICTs) and consumer demands. Smart grid technologies take the advantages of available modern technologies and their intelligent functionalities such as better situational awareness and operator assistance, autonomous control actions, efficiency enhancement, integration of renewable energy, improved market efficiency through innovative solutions, higher quality of services, etc. A conceptual model for smart grid systems is presented in Fig 1. This model consists of some actors such as generation, transmission, distribution, customer, service provider, operation center and markets.

Todays, smart grid systems are frequently used in developed countries. Although traditional power systems present one-way power transmission, a smart grid system provides two-way power flow and management of smart grid data. Data is accepted as "the new oil" and therefore producing new values from smart grid data is very important for organizations, communities, governments and also nations.

Smart grid system provides many advantages, however, it brings many security issues and risks in the implementation, application and operation of smart grids [1-5]. Smart grid systems are critical infrastructures and mainly targets of cyber attackers. In order to minimize security risks and prevent cyber threats, some measures are always required.

Cyber security issue is one of the main problems of smart grid systems that affect the sustainability and security of the whole system. However, there are a lot of challenges which make smart grid security more challenging such as new communication requirements, heterogeneous technologies, protocols and assets, proprietary systems, legacy devices, future threats and diverse subsystems [12]. In

addition, with the development of technology, cyber threats are changing, evolving and becoming more powerful. Hence, creating or developing exact solutions to these threats is a challenging problem. But providing maximum security for smart grid is the main task to maintain the grid more efficiently.

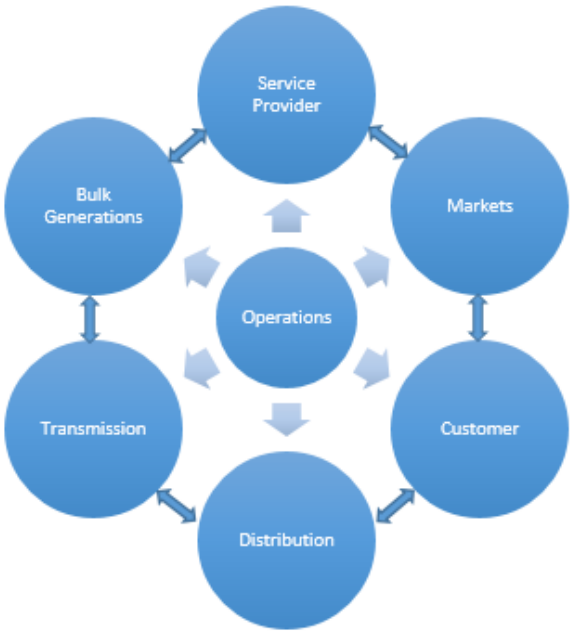


**Fig. 1.** Smart grid conceptual model [3]

Lots of cyber security technologies available today are used to protect smart grid systems against cyber attacks [5]. A smart grid system requires a purpose-built security architecture designed to protect confidential customer data and privacy of data about smart grid system. For example, NIST interoperability framework plays an important role and establishes policies and oversight structures for execution of cyber security controls [2].

In the literature, some papers were especially focused on network security for smart grid systems, because they report that providing the security of smart grid network is a challenging problem [8]. However, security concept in smart grid systems must be considered widely in all subsystems and components. Because all of the assets under these systems are in communication with each other and this case brings front many security issues.

In this paper, we reevaluated cyber attack risk assessment for smart grid in depth, provided an updated version of this assessment and briefed some current security standards for smart grid. Then we classified smart grid components into six categories and then comprehensively listed the existing vulnerabilities and threats for these components, for the first time. Finally, we presented some solutions and suggestions for smart grid security.

This paper was organized as follows. In Section 2, information security basics and risk evaluations for smart grid systems were presented. Security standards for smart grid systems were briefed in Section 3. Section 4 introduces the types of vulnerabilities and threats on smart grid systems. Cyber security solutions for smart grid systems were presented in Section 5. Finally, some remarks and conclusions were conducted in Section 6.

## 2. Information Security Basics and Risk Evaluations

Information security has three basic principles, which are known as Confidentiality, Integrity and Availability (CIA). Confidentiality is about to protect information from unauthorized disclosure. Integrity is maintaining and assuring the accuracy and completeness of data during transmitting, transferring, storing and analysing. Availability is the situation of being available of data when it is needed [6].

When the CIA principles are reconsidered for smart grid system, the following evaluations can be done [7]. Confidentiality is a user or operator side requirement that guarantees only authorized person can see the smart grid data; integrity is preventing any unauthorized manipulation or modification of smart grid data and availability is being available of smart grid data for authorized users. In order to prevent or minimize any malicious intents on smart grid systems, these principles should be widely evaluated and implemented carefully.

Smart grid systems consist of numerous subsystems and assets such as power generations, distributions, consumers, substation, communication and networking devices, intelligent electronic devices, human-machine interfaces, log servers, protocol gateway, smart meters, etc. The variety and complexity of these subsystems and assets present that the legacy cyber security techniques will not be sufficient to meet the requirements of whole infrastructure security while operating, monitoring and controlling data flow [6, 11]. However, these systems are very crucial and play important roles. Therefore, it is inevitable that these systems can be exposed to cyber attacks and malicious intents [9, 10].

In order to present a relationship between smart grid systems and cyber security, a cyber attack risk assessment was established in [6]. The concept of risk assessment was constructed by using three factors, which are threats, vulnerabilities and smart grid assets. Smart grid assets are the devices and components used in smart grid systems, vulnerabilities are the security gaps enabling malicious persons or cyber attackers to exploit the system and threats are the attacks from insiders or outsiders.

A simple risk evaluation was presented in [6], but, we re-evaluated and updated this concept and provided a new perspective to indicate the relation between risks and cyber security.

Let S1, S2 and S3 be the sets of threats, vulnerabilities and smart grid assets, respectively. Assume S1 ={Inside, Outside and Other Threats}, S2={Vulnerabilities in Systems} and S3={Smart Grid Assets}. Let R1, R2, R3 and R4 be the risk levels which are calculated as below;

$$R1 = \{S1 \cap S2\} \setminus R4 \quad (1)$$

$$R2 = \{S1 \cap S3\} \setminus R4 \quad (2)$$

$$R3 = \{S2 \cap S3\} \setminus R4 \quad (3)$$

$$R4 = \{S1 \cap S2 \cap S3\} \quad (4)$$

If we sort the risk levels in order, we obtain:

$$R4 > R3 \equiv R2 > R1 \quad (5)$$

From Eq. 5, it can be clearly seen that R4 is bigger than the others. It means that all smart grid assets are under security violations when vulnerabilities and threats occur in the system in the same time. Improved risk evaluation is presented in Fig 2.

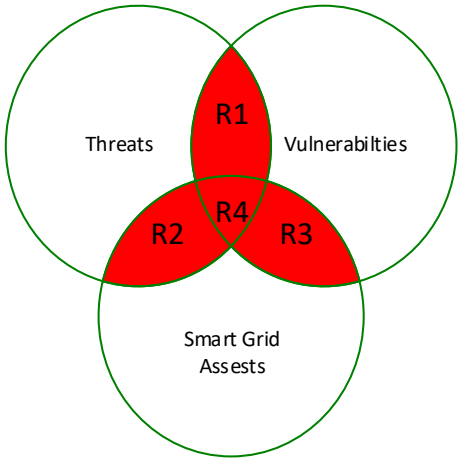


**Fig. 2.** Improved version of risk levels

## 3. Security Standards for Smart Grid

Implementing security standards for smart grid systems are extremely important to ensure a highly secure, scalable, consistently deployed smart grid systems [3]. IEC Strategic Group on Smart Grid, Technical Committees and their Subcommittees of IEEE Power & Energy Society, National Institute of Standards and Technology (NIST), National Standards of P.R.C for Smart Grid are the organizations supporting smart grid standardization. Some of the security standards are briefly explained below [13-16, 22, 23, 24] and a comprehensive list can be found in [24].

- "NIST Interagency Report 7628 for Smart Grid Cyber Security Strategy and Requirements" includes cybersecurity risk management framework and strategy, privacy and smart grid, logic interface analysis and advanced metering infrastructure security requirements.
- "IEC 61850 & GB/T22239 Security Classified Protection Standards", include data modelling, reporting schemes, fast transfer of events, setting groups, sampled data transfer, commands and data storage, and information security technology baseline for classified protection of information systems.
- "IEC 62351 on Smart Grid Security" is about data and communication security on smart grid systems.
- "ISO/IEC 1540 & GB18336 Security Assessment Standards" include security techniques, criteria for information security, security functional and assurance requirements and smart grid security assessments.
- "ISO 27001 & GB/T22080 Information Security Management Standards" are guidance for establishing governance and controlling security activities.
- "ITU-T.X.805" is a security architecture for systems providing end-to-end communications.
- "IEEE 1686-2007" is a standard for Substation Intelligent Electronic Devices Cyber Security Capabilities.
- "AMI System Security Requirements" focuses on security of advanced metering infrastructure.
- "NERC CIP Standards 002–009" are the standards for entities responsible for the availability and reliability of the bulk electric system.
- "NRC RG 5.71" is a standard for securing nuclear infrastructures.
- "EI RM Checklist" is a standard for risk management in energy facilities.
- "IEC 62443" is a standard for securing industrial automation and control systems.
- "IEC 27019" is a guidance based on ISO/IEC 27002:2013 and applied to process control systems used by the energy utility industry.
- "IEC 62541" is a general security standard for OPC Unified Architecture.

## 4. Vulnerabilities and Threats on Smart Grid System

Vulnerabilities may allow attackers to penetrate into networks, gain access to control software and modify or change the normal operations of the smart grid systems. Detailing and listing all vulnerabilities on smart grid systems is important to determine security requirements. In the literature, there exists many approaches and solutions to mitigate these vulnerabilities [17]. However, new vulnerabilities are being discovered in the systems, day by day.

Smart grid systems may have different types of vulnerabilities or threats due to using different protocols, containing many assets, communications among generators and transmissions, distributions and consumptions, transmissions and distributions, etc. [3, 9, 25].

In this paper, we categorized a smart grid system into six components, which are network, server, operator/user, hardware, software and data, and then evaluated cyber security for these components, separately. These categories are shown in Fig 3.

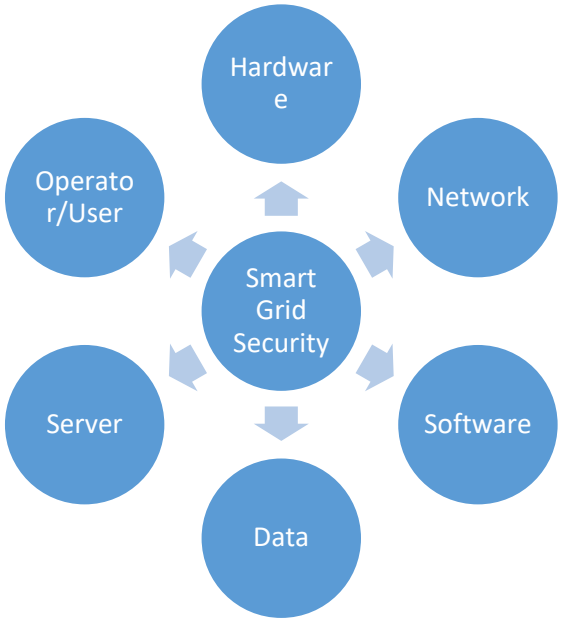


**Fig. 3.** Main components of smart grid systems

As reported in [7], smart grid systems have some potential security risks that must be addressed and some of these risks are listed below;

- Large number of network connections increase security vulnerabilities,
- Complexity helps hackers to attack the systems easily,
- Using new technologies or adding new components to the systems introduces new cases in security issues,
- Any grow and enlargement in smart nodes can cause DoS, DDoS, etc.

Common vulnerabilities encountered in the references [1, 5, 8, 10, 18-20] during this study were borrowed, reviewed and then rearranged according to the six main components of smart grid. Vulnerabilities that can be occurred on Network, Server, Software, Hardware, Operator/User and Data are listed in Table 1.a, Table 1.b, Table 1.c, Table 1.d, Table 1.e and finally Table 1.f, respectively.

**Table 1.a.** The list of vulnerabilities on Network

| No | Type of Vulnerability | Definition |
|---|---|---|
| A1 | Inappropriate or default security configurations | wrong policies or weak administration password |
| A2 | Authentication mechanism vulnerabilities | simple authentication policies, weak encryption |
| A3 | Using different protocol | even if using IP in network components of smart grid systems provides a big advantage, the systems have other protocol used in the systems |
| A4 | Misconfiguration | configuration flaws may cause attackers to gain access to the system and network |
| A5 | Design flaws | an attacker can gain high privileges because of design flaws in order to exploit vulnerabilities |
| A6 | Incorrect permission | an attacker might be able to bypass security restrictions because of insecure default permissions |
| A7 | Improper access control | control system mechanism fails to make a correct access control |
| A8 | Incorrect default permissions | leads unauthorized access to restricted areas |
| A9 | Improper user permissions | causes system users to perform actions that they should not be allowed |
| A10 | Missing authentication for critical function | missing authentication for functions which plays important roles on the systems leads crucial consequences |
| A11 | Improper restriction of excessive authentication attempts | huge number of login attempt may cause the system out of services |
| A12 | Unprotected transport of credentials | different attack types are developed to capture credentials while it is transported from one to another place |
| A13 | Lack of network segmentation | enables creating security zones which facilitate access control by separating system systems with different security policies and requirements |
| A14 | Lack of firewalls | network-based security system required to control inbound and outbound network traffic that detects malicious actions on the network |
| A15 | Lack of security audits | assessment of the system security helps the operator to take measure against |

| | | |
|---|---|---|
| | | attacker actions |
| A16 | Lack of or poor monitoring of IDSs | a comprehensive IDS deployment different methods for each domain to be monitored |
| A17 | Network devices not properly configured | improper configurations bring vulnerabilities |

**Table 1.b.** The list of vulnerabilities on Server

| No | Type of Vulnerability | Definition |
|---|---|---|
| B1 | Inappropriate or default security configurations | wrong policies or weak administration password |
| B2 | Authentication mechanism vulnerabilities | simple authentication policies, weak encryption |
| B3 | Misconfiguration | configuration flaws may cause attackers to gain access to the system and network |
| B4 | Incorrect permission | an attacker might be able to bypass security restrictions because of insecure default permissions |
| B5 | Improper access control | control system mechanism fails to make a correct access control |
| B6 | Incorrect default permissions | leads unauthorized access to restricted areas |
| B7 | Improper user permissions | causes system users to perform actions that they should not be allowed |
| B8 | Missing authentication for critical function | missing authentication for functions which plays important roles on the systems leads crucial consequences |
| B9 | Improper restriction of excessive authentication attempts | huge number of login attempt may cause the system out of services |
| B10 | Poor patch management | in time, system components may need patch operations which narrows the path of the attacker |
| B11 | Insufficiently protected credentials | improper protected credentials are golden opportunities for malicious persons to exhaust system resources and information |
| B12 | Plaintext storage of a password | a critical vulnerability provides attacker to gain access if he obtains the plaintext form of the password |
| B13 | Lack of logging | logging of the system events provides to detect security violations performed by malicious person |
| B14 | Poor logging practices | security violations may not be rapidly detected if logging mechanism is weak |
| B15 | Lack of security audits | assessment of the system security helps the operator to take measure against attacker actions |

**Table 1.c.** The list of vulnerabilities on Software

| No | Type of Vulnerability | Definition |
|---|---|---|
| C1 | Inappropriate or default security configurations | wrong policies or weak administration password |
| C2 | Insufficient security functions of application software | lack of secure coding, missing session control, availability to DoS attacks |
| C3 | Authentication mechanism vulnerabilities | simple authentication policies, weak encryption |
| C4 | Misconfiguration | configuration flaws may cause attackers to gain access to the system and |

| | | |
|---|---|---|
| | | network |
| C5 | Design flaws | an attacker can gain high privileges because of design flaws in order to exploit vulnerabilities |
| C6 | Insufficient input validation | program fails to validate input |
| C7 | Incorrect permission | an attacker might be able to bypass security restrictions because of insecure default permissions |
| C8 | Improper access control | control system mechanism fails to make a correct access control |
| C9 | Incorrect default permissions | leads unauthorized access to restricted areas |
| C10 | Improper user permissions | causes system users to perform actions that they should not be allowed |
| C11 | Missing authentication for critical function | missing authentication for functions which plays important roles on the systems leads crucial consequences |
| C12 | Improper restriction of excessive authentication attempts | huge number of login attempt may cause the system out of services |
| C13 | Poor patch management | in time, system components may need patch operations which narrows the path of attacker |
| C14 | Weak testing environments | a poor test of software may harbor different unnoticeable flaws or vulnerabilities |
| C15 | Limited patch management policies | limited patch management policies make the system less secure against attacker |
| C16 | Lack of security audits | assessment of the system security helps operator to take measure against attacker actions |

**Table 1.d.** The list of vulnerabilities on Hardware

| No | Type of Vulnerability | Definition |
|---|---|---|
| D1 | Large number of intelligent devices | smart grid systems include huge number of devices that are involved in electricity supply, management and control with support of ICTs |
| D2 | Physical security | many components of smart grid systems are out of utility's premises. This situation causes insecure physical locations and vulnerable physical access |

**Table 1.e.** The list of vulnerabilities on Operator/User

| No | Type of Vulnerability | Definition |
|---|---|---|
| E1 | Different team's backgrounds | inefficient and insufficient communications among teams might cause interoperability problem and bad decisions and opinions about the system that leads emergence of vulnerabilities |
| E2 | More stakeholders | stakeholders used different technologies, protocols and policies so this causes more security risks not only from outsider but also insider attacks |
| E3 | Indiscretions by Personnel | training of personnel is important to avoid illegal behavior such as unauthorized interception of private communication |

**Table 1.f.** The list of vulnerabilities on Data

| No | Type of Vulnerability | Definition |
|---|---|---|
| F1 | Unprotected personal identifiers | unprotected smart grid data containing personal identifiers cause privacy breaches |
| F2 | Lack of data security | an attacker may change the real value of data |

According to the tables presented above, it can be seen that there exist many vulnerabilities on the six components of smart grid and it is a challenging issue to provide security on smart grid. While the number of vulnerabilities change from component to component, it must be kept in the mind that even any of these vulnerabilities enables attackers to give great damages to systems.

In addition, threats targeting smart grid systems are borrowed from the references [5, 8, 10, 18, 19, 21], reviewed, rearranged and then grouped according to the six main components of the smart grid. Threats targeting the components of Network, Server, Software, Hardware, Operator/User and Data are listed in Table 2.a, Table 2.b, Table 2.c, Table 2.d, Table 2.e and finally Table 2.f, respectively.

**Table 2.a.** The list of threats on Network

| No | Type of Threat | Definition |
|---|---|---|
| G1 | Tampering | modifying system operator control commands causes system failures. |
| G2 | Replay | attackers replay system operator control commands results in system malfunction |
| G3 | Eavesdropping | attackers steal system credential of the administrator by sniffing the network |
| G4 | Network monitoring, discovery and analysis | attackers monitor the network and discover vulnerabilities of the systems via available vulnerabilities |
| G5 | DoS | DoS attacks aim to damage availability of the system and interrupt the system normal operation |
| G6 | Spoofing | it is the process of masking IP address of metering device to manipulate or modify accounts. |
| G7 | Intrusion attacks | an attack type on compromise of confidentiality and in another word illegal access to systems in order to control and perform malicious actions |
| G8 | Insider attack | some malicious insider may want to leak secrets or sensitive information and harm to the systems |
| G9 | Man in the middle | an attack type that attacker secretly intervene two parties and intends to capture data flow between parties |

**Table 2.b.** The list of threats on Server

| No | Type of Threat | Definition |
|---|---|---|
| H1 | Viruses, Spyware, Trojans and Worms | operating system, databases and applications may have security vulnerabilities that cause attackers to access the systems and destruct applications and control systems |
| H2 | Origin Disguise | a disguised operator may want to control a system subfunction to damage the system, or by phishing e-mails attackers may obtain users personal information and disguises user identity to control system devices |
| H3 | Tampering | modifying system operator control commands causes system failures. |
| H4 | Replay | attackers replay system operator control commands results in system malfunction |
| H5 | Keylogging | monitoring keystrokes from operators are to obtain credential information |
| H6 | Deletion of system files on server | system files can be deleted from servers by intruders or malicious employees. |
| H7 | Intrusion attacks | an attack type on compromise of confidentiality and in another word illegal access to systems in order to control and perform malicious actions |
| H8 | Insider attack | malicious insider may want to leak secrets or sensitive information and harm to the systems |
| H9 | Theft | a type of attack that one may want to obtain special information about the system and users information illegally |
| H10 | Trapdoor | an entry place that inserted by a programmer into computer program allows him to secret |

| | | |
|---|---|---|
| | | access to the program or system |
| H11 | Resource Exhaustion | malicious person uses up available resources hence works or processes on these resources cannot be accomplished |
| H12 | Phishing | is the attempt to acquire sensitive information such as username and password by sending fraudulent email messages appearing to come from a legitimate enterprise |
| H13 | XSS | enables attackers to inject client-side script to perform malicious actions |
| H14 | Operating system command injection | a type of attack that allows attackers to execute arbitrary command on host |
| H15 | Path traversal | an attacker can access the files and directories stored out of web root folder |

**Table 2.c.** The list of threats on Software

| No | Type of Threat | Definition |
|---|---|---|
| I1 | Tampering | modifying system operator control commands causes system failures. |
| I2 | Replay | attackers replay system operator control commands results in system malfunction |
| I3 | Keylogging | monitoring keystrokes from operators are to obtain credential information |
| I4 | Insider attack | some malicious insider may want to leak secrets or sensitive information and harm to the systems |
| I5 | Trapdoor | an entry place that inserted by a programmer into computer program allows him to secret access to the program or system |
| I6 | Web compromise | using vulnerabilities in a website or web application to further an attack |
| I7 | Buffer overflow | lack of a correct design of software in code wise that emerges when attacker write more data to available allocated memory |

**Table 2.d.** The list of threats on Hardware

| No | Type of Threat | Definition |
|---|---|---|
| J1 | Physical intrusion | people may physically intrude into smart meter to perform unauthorized actions |

**Table 2.e.** The list of threats on Operator/User

| No | Type of Threat | Definition |
|---|---|---|
| K1 | Origin Disguise | a disguised operator may want to control a system subfunction to damage the system, or by phishing e-mails attackers may obtain users personal information and disguises user identity to control system devices |
| K2 | Social engineering attacks | nontechnical attack type that aims to gain trust of users to obtain credential to log on into system |
| K3 | Phishing | is the attempt to acquire sensitive information such as username and password by sending fraudulent email messages appearing to come from a legitimate enterprise |
| K4 | Information disclosure | unauthorized access to sensitive information by malicious person |
| K5 | User compromise | gaining unauthorized use of user privilege |
| K6 | Root compromise | gaining unauthorized use of administrator privilege |

**Table 2.f.** The list of threats on Data

| No | Type of Threat | Definition |
|---|---|---|
| L1 | Disclosure | attacker may disclose the owner of data with sensitive attributes |
| L2 | Violation of data completeness | the integrity of data may be violated |

According to the tables given above, it can be seen that there are many threats targeting smart grid security. Hence, security experts should take some measures to defeat these threats and make the system more secure.

## 5. Cyber Security Solutions for Smart Grid

In order to achieve better security, smart grid structures should have appropriate and tight security measures. Strong authentication and cryptographic infrastructure are required for all devices, meters, components and communications. Public Key Infrastructure (PKI) technology is a useful measure to make more secure smart grid system. When PKI is applied on smart grid systems, five main technical elements have been encountered [3]. These are:

- PKI Standards help to establish requirements of security operations of energy service providers such as utilities, generators, smart grid device manufacturers, etc.
- Smart Grid PKI Tools is employed to make easier implementation of PKI in smart grid.
- Device attestation is used to define or discover devices and their true identities on the network.
- Trust Anchor Security is used to manage trust relationships. Because of having huge number of devices in smart grid, an effective and comprehensive Trust Anchor Mechanism System is also needed.
- The Certificate Attributes facilitates high availability needed for the power grid.

In addition, appropriate network connectivity, smart grid security services and protocols, and identity management are some suggestions to make smart grid system more secure and complete [3]. These are summarized below:

- Appropriate network connectivity must be established against to malicious actions such as interruption, modification and fabrications.
- Robust firewalls, intrusion detection and prevention systems must be used to increase security level or minimize attacks from insiders and outsiders.
- Smart grid security service units lead network operators about identifying, controlling and managing security risks and satisfy per utility's needs properly.
- Protocols and identity management are important to manage authentications and authorization status.

ISO/IEC 27000 series and Information Security Forum (ISF) are two important programs about information security for every organization. Role-based authorization, user authentication and intrusion detection systems are the other methods that are employed in defense solutions at different smart grid security levels which are classified in [6] as data, application, HAN, NAN and WAN.

DoS attack is one of the most popular malicious actions on smart grid systems. The propose of and DoS attacks is to interrupt or halt the systems. Experts might detect these attacks in four methods, which are signal-based, packet-based, proactive and hybrid. Signal-based methods compare signal strength to a threshold value that generates an alarm. Packet-based methods control transmission results which can be ended with failure. Proactive method sends probing packets to test or define potential attacker. Hybrid method combines various methods to detect any attack. Additionally, cryptographic methods such as encryption, authentication and key management enables to reduce the risk of cyber attacks on smart grid systems [12].

## 6. Remarks and Conclusions

Smart grid systems consist of huge number of components or subsystems. They are critical infrastructures and require monitoring, managing, processing, controlling and securing data and systems. These systems are usually main targets of hackers, malicious persons or attackers.

In this paper, vulnerabilities and threats on smart grid systems was reviewed, categorized according to six main components of smart grid, criticised in security perspective and some suggestions were presented. The contributions and suggestions of this article are summarised below:

- The results have shown once more that, in general, securing smart grid systems is getting difficult with high risks because of having many protocols, standards, policies, components, systems, blocks, etc. Obviously, due to enlargement of smart grid systems, these systems require more secure platforms more than today. Even if ICT based systems have more vulnerabilities than smart grid systems, it should be always kept in mind that these systems are critical systems and should be protected better than other systems.
- As summarized earlier, there exist many standards and solutions for smart grid systems, but it still needs more attention because of the nature of the systems containing vulnerabilities, attacks, risks, threats, etc. and their continuous increments. Smart grid system security covers many security perspectives inside such as data (big data, smart data, etc.), application, protocols (HAN, NAN, WAN, BAN, IAN, etc.), communication, hardware, software, policies, integration, management, data storage, national/international laws, privacy issues, cyber attacks, vulnerabilities, threats, social engineering, etc. All these security risks should be considered for defending these

systems, networks, components, blocks, etc. Due to those, standards must be first applied, implemented and kept updated based on developed technologies, strategies, methodologies and encountered security risks.

- Using old devices, components, software, networks, systems in the systems is also main issues to address for better risk management and keep the systems more secure. Hence, old devices, components, software, networks, systems should be updated or replaced based on security policies and security mechanisms. Due to large and complex structures of the systems, security configurations of the systems are not set properly or not controlled so more attention is to be paid for proper settings. Physical security is also another issue to be considered in insecure physical locations.

- IEEE standards named in the NIST Framework and Roadmap especially, IEEE Smart Grid Series Standards of 2030 and 1547 should be focused on.

- Not only IEEE but also the security standards provided by ITU, ISACA, ISO/IEC, ETSI, PCI, NIST, NERCS, PCKS, ENISA should be also utilized for security of smart grid systems.

- Recent technologies such as Artificial Intelligence, Big Data Analytics, Block Chain, etc. should be also the recent topics to provide better security in smart grid systems. For example, securing smart grid platforms using block chain, analysing variety of smart grid data with big data analytics and developing an intelligent alert system for smart grid security are the topics to be concentrated for the future developments.

- Frameworks provided by NIST, ISACA, PKI, PCIDSS, ISO27001, CIS Critical Security Controls should be also taking into account to provide better security in broad sense.

- Interoperability is another important topic to be sorted it out in smart grid systems and environments due to having large components, devices, protocols, systems and networks. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0" is a very good guideline having with many examples. As also summarized in this article, the number of smart grid-specific standards are too little and new and comprehensive standards should be established, updated or released.

- Vulnerabilities and attacks mentioned in previous works should be centered on smart grid. Defense solutions combined and presented should be focused on. Defense solutions for smart grid systems must be extended to its subsystems, from bottom to top, and from the specific to the general or vice versa, it must be evaluated with a broad horizon and perspective.

- Smart grid systems require comprehensive security architectures that play a crucial role in providing better or higher security. Available systems should be revised in consideration with this perspective.

- In order to reduce the risk, vulnerable systems should be cleaned or replaced with the developed and hygiene technologies or solutions, due to old or new technologies, misconfiguration, bad management, lack of security policies and procedures or lack of proper auditing, etc.

- Radio frequency based communication instead of IP might be preferred to make the system less vulnerable to attacks as applied in Taiwan, as an alternative solution.

- It is also better to share the experiences and good or bad practices among the countries to protect the systems more efficiently. Especially, sharing experiences of Computer Emergency Response Teams (CERT) responsible for taking measures and maintaining national cybersecurity against cyber attacks is very important to provide better and in time security. It should be always considered that this issue is not only national level but also international level to overcome the problems encountered in smart grid as quick and much as possible.

- Global Cybersecurity Index proposed by ITU (International Telecommunication Unit 2016) is a measure for protection and good comparison. This issue is also taken into account for better smart grid systems in all countries.

- It needs to be stressed once more that there have been many vulnerabilities and attack types targeted to smart grid systems. The numbers of malicious actions and threats increase with the developed new technologies and solutions integrating and implementing these into available systems and networks so those are should be the issues to be considered and developed new test systems.

- To protect smart grid systems, the solutions summarized in this article should be considered, applied, implemented and audited.

- Finally, it is expected that solutions and suggestions proposed in this article may guide security administrators, experts, users, developers, manager of institutions or companies to handle grid systems smartly and to secure against malicious actions, attacks, codes and systems.

## References

[1] F. Aloul, A. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy,* vol. 1, pp. 1-6, 2012. (Article)

[2] J. Farquharson, A. Wang, and J. Howard, "Smart grid cyber security and substation network security," in *Innovative smart grid technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-5. (Conference Paper)

[3] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Innovative Smart Grid Technologies (ISGT), 2010*, 2010, pp. 1-7. (Conference Paper)

[4] K. Moslehi and R. Kumar, "Smart grid-a reliability perspective," in *Innovative Smart Grid Technologies (ISGT), 2010*, 2010, pp. 1-8. (Conference Paper)

[5] J. Anu, R. Agrawal, C. Seay, and S. Bhattacharya, "Smart Grid Security Risks," in *Information Technology-New Generations (ITNG), 2015 12th International Conference on*, 2015, pp. 485-489. (Conference Paper)

[6] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*, 2015, pp. 1-6. (Conference Paper)

[7] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on*, 2011, pp. 1-4. (Conference Paper)

[8] X. Liang, K. Gao, X. Zheng, and T. Zhao, "A Study on Cyber Security of Smart Grid on Public Networks," in *Green Technologies Conference, 2013 IEEE*, 2013, pp. 301-308. (Conference Paper)

[9] B. Buluc and H. I. Bulbul, "Increasing Social Awareness of Consumer Behaviors On Smart Grids Energy Systems," *International Journal of Renewable Energy Research (IJRER),* vol. 6, pp. 1588-1592, 2016. (Article)

[10] I. Dumitrache and D. I. Dogaru, "Smart Grid Overview: Infrastructure, Cyber-Physical Security and Challenges," in *Control Systems and Computer Science (CSCS), 2015 20th International Conference on*, 2015, pp. 693-699. (Conference Paper)

[11] B. Al-Omar, A. Al-Ali, R. Ahmed, and T. Landolsi, "Role of information and communication technologies in the smart grid," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 3, pp. 707-716, 2012. (Article)

[12] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. Nicolae Borza, "Smart grid security issues," in *Compatibility and Power Electronics (CPE), 2015 9th International Conference on*, 2015, pp. 534-538. (Conference Paper)

[13] Y. Wang, D. Ruan, D. Gu, J. Gao, D. Liu, J. Xu*, et al.*, "Analysis of smart grid security standards," in *Computer science and automation engineering (CSAE), 2011 IEEE international conference on*, 2011, pp. 697-701. (Conference Paper)

[14] (04.12.2018). *ITU-T Recommendations by Series*. Available:http://www.itu.int/itu-t/recommendations/index.aspx?ser=X

[15] E. Lebanidze, "Guide to Developing a Cyber Security and Risk Mitigation Plan," *The National Rural Electric Research Network,* 2011.

[16] The Smart Grid Interoperability Panel–Cyber Security Working Group, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," *NIST Special Publication,* vol. 154, 2010.

[17] A. Özbilen, "Security and Solution Proposals for TCP/IP Based Distributed Industrial Control Systems," PH. D., Department of Electric Education, Gazi University, Graduate School of Natural and Applied Sciences, 2012.

[18] K. A. Ahmed, Z. Aung, and D. Svetinovic, "Smart grid wireless network security requirements analysis," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, 2013, pp. 871-878. (Conference Paper)

[19] I. Ghansah, "Smart grid cyber security potential threats, vulnerabilities and risks," *California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047,* 2009.

[20] T. Nelson and M. Chaffin, "Common cybersecurity vulnerabilities in industrial control systems," *Control Systems Security Program,* 2011.

[21] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A cyber attack taxonomy," *Annual Symposium on Information Assurance,* 2009, pp. 2-12. (Conference Paper)

[22] S. Hussain, M. Meraj, M. Abughalwa and A. Shifka, "Smart Grid Cybersecurity: Standards and Technical Countermeasures", in *International Conference on Computer and Applications,* 2018, pp. 136-140. (Conference Paper)

[23] K. C. Ruland, J. Sassmannshausen, K. Waedt and N. Zivic, "Smart grid security – an overview of standards and guidelines ", *Elektrotechnik & Informationstechnik,* vol. 134, pp. 19-25, 2017. (Article)

[24] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey", *Computer Standards and Interfaces,* vol. 56, pp. 1-18, 2018. (Article)

[25] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, C. Covrig, "A survey on the critical issues in smart grid technologies", *Renewable and Sustainable Energy Reviews,* vol. 54., pp. 396-405, 2016. (Article)