Mikthan Security Technologies Limited
S. Coast Hwy Suite 1119,
Laguna Beach 92651 California USA
info@mikthansecurity.com
+1(714) 716-1117

Review Article

Cyber Security for Smart Energy, Cryptography, and Privacy

The invention of “smart grid” promises to improve the efficiency and reliability of the power system. As smart grid is turning out to be one of the most promising technologies, its security concerns are becoming more crucial. The grid is susceptible to different types of attacks. This paper will focus on these threats and risks especially relating to cyber security. Cyber security is a vital topic, since the smart grid uses high level of computation like the IT. We will also see cryptography and key management techniques that are required to overcome these attacks. Privacy of consumers is another important security concern that this paper will deal with.

1. Introduction

One of the most important, complex, and intelligent network we have is the “power system”. This system consists of cir-cuits, wires, towers, transformers, sensors, and cables inter-linked to provide us with uninterrupted power supply. This system is mainly a mechanical system and has very little elec-tronics associated with it like sensors and communication. However, as technology has progressed rapidly and almost all the latest devices need electricity for their operation, it is necessary that we make our present power system more re-liable and efficient [1].

We can say the demand for electricity is greater than its supply. The demand is not only high but also fluctuating. We could rely on renewable resources like solar energy and wind energy to meet the present need, but unfortunately, they turn out to be fluctuating too.

The smart grid enhances the functionality of the power delivery system. This is possible because smart grid uses sensors, communications, computation, and control in order to make the system smart and by applying intelligence to it in the form of control through feedback or in other words by using two way communication. In order to utilize the available resources, consumers need to change, and they need to act more “smart”. They have to change from being passive consumers to being active consumers [1]. Smart grids aim to reduce the energy consumption, ensure reliability of power supply, reduce carbon foot print, and minimize the costs associated with power consumption.

The smart grid system has many advantages, one of them being cost effectiveness. This is because the grid uses internet for communication purpose. However, using the internet means vulnerability to cyber attacks. As opposed to the original power system, the smart grid uses ethernet, TCP/IP and other operating systems, thus making the grid more susceptible to attacks. The smart grid should enhance the security of the power system, but protecting the grid is a more challenging task now. Once the system is attacked, the attacker may control several meters or disrupt the load balance of the system. Thus, we need to gain complete knowledge about cyber security, so we can eliminate it com-pletely. We also need to focus on the cryptographic methods proposed by the National Institute of Standards and Technol-ogy (NIST) in order to avoid these cyber attacks.

In this paper, we will study smart grid security in more depth. The goal of this paper is to cover the security challenges related to cyber security, and we will also study how cryptography is used in order to eliminate cyber attacks. Finally, we will also discuss in brief privacy which is another smart grid security concern. The rest of the paper is organized as follows. We start by reviewing the challenges and goals of smart grid in Section 2. This is followed by the smart grid architecture in Section 3. We focus on cyber security in Section 4. Section 5 explains cryptography used

for smart grid security in depth. Privacy in context with smart grid security is explained in Section 6. And finally, we conclude in Section 7.

2. The Smart Energy: Goals and Challenges

2.1. Goals. The present power grid has more than 9200 elec-tric generating units, 1,000,000 plus megawatts of generating capacity connected by using 300,000 miles of transmission lines [2].

Electricity has one basic requirement; it needs to be utilized as soon as it is generated. The present grid does so successfully. However, now, the grid is overburdened. The reliability of the present grid is at stake, and this can be seen, since we have been witnessing more brownouts and black-outs recently.

Another thing that needs to be addressed when we consider the present grid is the efficiency. By making the grid more efficient, we can save millions of dollars. There is also a reverse case here; if there is an hour of power outage, the nation loses a tremendous amount of money. Electricity needs to be more affordable too. The rate of electricity is increasing gradually which makes it less affordable.

Majority of the electricity produced in the United States of America comes by burning coal. The carbon footprints that occur due to this contributes to global warming. If we introduce the use of renewable energy in our grid, we can reduce the carbon footprint.

We also need to compete globally with other countries that have better technology for energy distribution.

And finally, the grids security is of major concern. The current grid has a centralized architecture, and thus making it more vulnerable to attacks. A failure can hamper the country's banking, traffic, communication, and security system [2].

Thus, we introduce the smart grid system (Figure 1). We now have a smart power grid that creates a link between elec-tricity, communications, and computer control. Many coun-tries are actively participating in the development of smart grid; for example, the ETP created a joint vision for the European network of 2020 [3] and beyond, and the US estab-lished a federal smart grid task force under the Department of Energy (DoE).

The aim is first to control the electricity supply with utmost efficiency and also reduce the carbon emissions. A smart grid system basically needs to have the following properties (Figure 2) [4]:

(1) digitalization,

(2) intelligence,

(3) resilience,

(4) customization,

(5) flexibility.

Digitalization means to have a digital platform which makes the system fast and reliable. Flexibility would mean that the smart grid needs to be compatible, expandable, and adaptable. Intelligence would mean to inherit an intelligent technology. Resilience would mean that the system should not be affected by any attacks. And lastly, customization means the system needs to be client tailored.

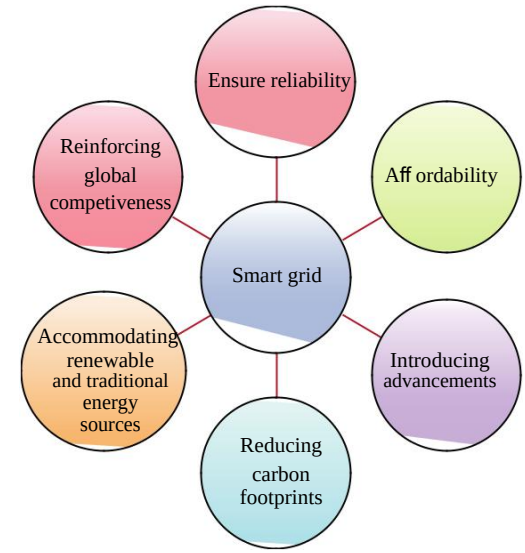

FIGURE 1: Smart grid goals.

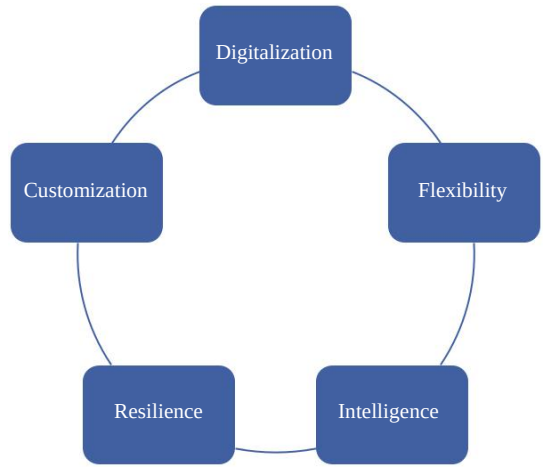

FIGURE 2: Smart grid properties.

The power grid today is already a very complex and intelligent system. It comprises thousands of miles of high voltage lines, an intelligent control system that controls it, and a communication system that distributes it. A smart grid would help us improve the efficiency and availability of the same power system by using better control strategies.

2.2. Challenges. Let us see what are the problems related to the current power grid system.

The current grid is "purpose built". This means that it is made in such a way that we cannot add any new control points and any security functions. The grid is bandwidth lim-ited, and this restricts us from adding any extra information that would be required to ensure authentication. If there is

no room for security, it implies the protocols runs relying on trust, and thus ignoring the possibility of any unknown entity.

In case of the new smart grid, the practice has changed; initially the devices used were purpose built, and these days, they are multipurpose. Instead of using dedicated lines for communication, we use the TCP/IP. Though the technology has drastically improved, the chances of being attacked have also increased rapidly.

Another issue is that smart meters would read the energy usage of a particular residence multiple times in an hour, which would lead to a loss of privacy for the consumer. That is because if one has a smart grid, then one can know whether a residence is occupied or not and also at what time what appliances are being used. This could lead to two different types of attack, either a simple theft or pricing the signals for monetary gains [5].

3. The Smart Energy Architecture

3.1. A General Model. The electricity delivery network basically consists of two subsystems, a transmission system and a distribution subsystem (Figure 3).

In the transmission network, electricity is moved in bulk from 345 kV to 800 kV over AC and DC lines. Power flows in one direction and is distributed to consumers at 132 kV. However, the smart grid will provide bidirectional metering unlike the present grid.

The grid includes a monitoring system and a smart meter which keeps track of the electricity consumed. It includes superconductivity transmission lines which help to reduce the resistive losses and also is compatible to other sources of energy like wind, solar, and so forth.

3.2. Functional Components. The three functional components of a smart grid are smart control centers, smart transmission networks, and smart substations. Let us take a look at them one by one as follows [4].

3.2.1. Smart Control Centers. The smart control centers will depend on the existing control centers. The main functions of a control center are as follows [4].

Monitoring/Visualization. The present control center performs monitoring based on the data collected via SCADA and RTUs (remote terminal units). In the future, information will be obtained from state measurement modules. It is better than the present module in terms of "running time" and "robustness". In the future, the outcomes will be combined with a wide area geographical information system (GIS), and a visual display will be provided. In this manner, more information will be covered. Also, in the future, the control centers will provide the root cause of a problem rather than just giving an alarming signal.

Analytical Capability. The future is expected to have online time domain-based analysis. These would include voltage stability and transient angular stability. The present grid

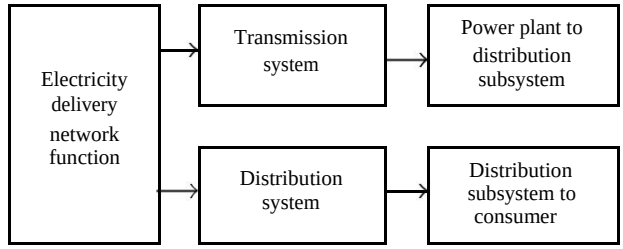

FIGURE 3: A general model.

does not provide the real-time dynamic characteristics of the system whereas in the future, we will have a dynamic model updates. Also, the future grid is expected to have a look ahead simulation capability.

Controllability. In the present grid, operations like separating, restoration, and so forth, depend on offline studies. In the future, these will be real time and dynamic. Fixed values are used for the protection and the control settings now, but in the future, proactive and adaptive approaches will be used. Also, there is no coordination when any decision is taken in the current technology. In future, there will be coordination in order to gain a better control.

Interaction with Electricity Market. The main aim of a smart grid system is to achieve high efficiency. For this, we need a control system that dynamically adjusts in accordance with the market. Sophisticated tools are used for this purpose. Also, the smart grid needs to accommodate renewable energy sources.

3.2.2. Smart Transmission Networks. There are new features that are included in the smart grid which involves signal processing, sensing, advanced materials, power electronics, communications and computing. These would improve the efficiency, utilization, quality, and security of the present system.

For long distance transmission, we use high-capacity AC and DC facilities. When the overhead lines are not possible, underground cables are used. High-temperature composite conductors and high-temperature superconducting cables are used for electrical transmission, since they have a higher current carrying capacity, low voltage drop, reduced line losses, light in weight, and better controllability. Six and twelve phase transmission lines are used which provide great-er power transmission with reduced electromagnetic field and great phase cancellation.

Flexible and reliable transmission is made possible by using advanced flexible AC transmission system (FACTS) and high-voltage DC (HVDC) devices. FACTS are placed in the transmission network, and they improve the dynamic performance and stability. They will help grid to be free from transmission congestions. HVDC is used as a cost-effective alternative to AC lines.

Intelligent sensors are used with advanced signal processing to measure the line parameters and monitor the status

around the sensor location. These sensors can detect the conductor temperature, detect galloping lines, predict initial failures of insulators and towers, identify fault locations, and so forth.

Based on these parameters, the operating conditions can be autonomously detected, analyzed, and responded in case of emergencies, thus maintaining the reliability and security of the transmission system. Also, smart grid systems have reduced catastrophic failures and less maintenance cost. Extreme event facility hardening systems are used to manage failure and restore the system rapidly [4].

3.2.3. Smart Substation. The equipments in the substation should be more reliable and efficient for functions like monitoring, controlling, operating, protecting, and maintaining. The main functions are the following [4]:

(1) smart sensing and measurement,

(2) communication,

(3) autonomous control and adaptive protection,

(4) data management and visualization,

(5) monitoring and alarming,

(6) diagnosis and prognosis,

(7) advanced interfaces with distributed resources,

(8) real-time modeling.

4. Cyber Security

4.1. Cyber Security Model. Like for any other network's security, the three main objectives that cyber security focuses on is availability, integrity, and confidentiality, that is, avail-ability of power with integrity of information and confiden-tiality of customer's information.

Availability. The reason why we have smart grid is "availability". The basic goal of our network is to provide uninterrupted power supply to the users and to match user requirements.

Confidentiality. The grid network is responsible for the protection of a user's information. If the data is not protected, ample information about the user can be revealed to the attacker.

Integrity. The messages received from the user end should be authenticated. The network must ensure the information is not tampered. Also, the source of message should be authentic.

The smart grid's cyber infrastructure consists of electronic information and communication systems and services along with the information contained in these systems and services. This includes both the hardware and software too. Their basic functions are to process, store, and communicate information. This is done using a control system (SCADA) [6, 7]. The SCADA is a neutral system.

4.2. SCADA System. Supervisory control and data acquisition (SCADA) systems are basically centralized control systems that are used by our power distribution system. It is used for monitoring and controlling process [8].

The main blocks that a SCADA system includes are the following:

(i) HMI (human machine interface) presents processed data,

(ii) a supervisory computer that collects all the data and uses it for processing purpose,

(iii) remote terminal units (RTUs),

(iv) programmable logic controller (PLC),

(v) communication infrastructure.

By using the power system communication in the smart grid, the SCADA systems are connected to other systems like the internet or by certain dedicated lines. The vendors are using off the shelf products as part of the SCADA systems. These products are similar to the personal computers we use at home, and thus are susceptible to attacks and different threats [9].

A SCADA system is a necessary element in the grid infrastructure. It is used for two purposes, first the public transport system and second the public control system.

The cyber security basically can be attacked in three steps [10] as follows:

(1) the attacker has control over the SCADA system,

(2) the attacker identifies the system to launch an intelligent attack,

(3) attacker initiates the attack.

These SCADA systems are most vulnerable to attacks. In order to prevent the attackers from gaining control of SCADA system, automation will be required. The NIST has established smart grid cyber security coordination task group (CSCTG) which addresses and evaluates processes leading to comprehensive cyber security policies for smart grid [6].

The risks assessed by the CSCTG include [6, 11] the following:

(i) complexity of grid leading to weak point and openings to attackers,

(ii) cascading errors as a result of interconnected networks,

(iii) DoS (denial of service) attack,

(iv) attack on consumer privacy to excessive data gather-ing,

(v) attacks from annoyed employees and terrorists,

(vi) as number of nodes increases the number of entry points for an attacker also increases.

In order to obtain cyber security, we also need to have a robust hardware. We can discuss this further by dividing the hardware section in two parts: (a) new substations and (b) existing systems. In case of new substations, we can

completely design the system to be immune against cyber security threats. For this, we can use managed switches. These are smart switches which perform multifunctions like access control, traffic prioritization, managing data flow, and so forth. However, since we already have an ethernet-based system laid, we must make changes to these systems such that they can withstand cyber attacks. For this, we can either update the present infrastructure or Install Se-curity appliances. Security appliances are present between the ethernet connections and are used for examining and monitoring purposes. Another addition to existing systems would be the use of firewalls. They block unauthorized access to any network and work according to the user defined rules. We could also use a technology called VPN (virtual private network), where the connection between two stations is secured [12].

The Cyberspace Policy Review initiated by President Obama advised that "the Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources." Specifically, the review recommended that as "the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks [11, 13]."

The Department of Energy should work with the federal energy regulatory commission to determine whether additional security mandates and procedures should be developed for energy-related industrial control systems. In addition, the United States deploys new smart grid technology, the federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks [11].

Chairman Thompson issued the following statement regarding the legislation: "Any failure of our electric grid, whether intentional or unintentional would have a significant and potentially devastating impact on our nation. We must ensure that the proper protections, resources and regulatory authorities are in place to address any threat aimed at our power system. This legislation addresses these critical issues by providing a common sense approach to ensure continued security of the nation's electric infrastructure [14],".

The security concerns are increasing as the numbers of connections are increasing. There have been cases where cyber spies from China, Russia, and other countries are reported to have entered the United States electrical grid and tried to attack the system. The ability to resist attacks is one of the inevitable functions of the smart grid [15].

5. Cryptography and Key Management

In order to obtain cyber security, we must secure data using cryptography and different keys. In this section, we will study the various aspects related to cryptography and key management. We will first go through the different constraints related to cryptography followed by the cryptographic issues and solutions [16].

5.1. Constraints

5.1.1. Computational Constraints. Residential meters will have limitations when it comes to computational power and the ability to store cryptographic materials. The future devices are bound to have the basic cryptographic capabil-ities including the ability to support symmetric ciphers for authentication. The use of low-cost hardware with embedded cryptography is necessary but not enough to achieve high availability, integrity and confidentiality in the smart grid.

5.1.2. Channel Bandwidth. The communications that will take place in a smart grid system will take place over different channels that have different bandwidths. AES is a cipher that produces the same number of output bits as input bits. These bits cannot be compressed too, since they are encrypted and random in nature. In case we need to compress this data, we need to do so before encryption. Another factor to be taken into consideration is the cipher-based message authentication code (CMAC), which is added as a fixed overhead to a message and is typically 64 bits or 96 bits. These overheads turn out to be significant when we are dealing with short messages, since they would need large channel Bandwidth.

5.1.3. Connectivity. Standard public key infrastructure-based on peer-to-peer key establishment model where any peer may need to communicate with another is not desirable from a security standpoint for components. Many devices may not have connectivity to key servers, certificate authorities, online certificate status, and protocol Servers. Many connec-tions between smart grid devices will have longer duration than typical internet connection.

5.2. General Cryptographic Issues

Entropy. Cryptographic key generation requires a good source of entropy that creates randomness which is unavailable for many devices.

Cipher Suite. A cipher suite that is open is needed in order to achieve interoperability. A decision about which block cipher, their modes, key sizes, and asymmetric ciphers forms the base of authentication operation.

Key Management Issues. Security protocols depend on secu-rity associations. There can be two types in which the security is authenticated: (1) use of Secret key and (2) use of certificate authority. In case we use secret keys, the keys have to be transported from a device to another. To transport these keys, we need a set of keys for each pair of communicating devices and all this needs to be well coordinated. There is also a hardware alternative for this, but

that is a costlier option and involves a large amount of overhead. Digital certificates turn out to be cost effective solution as coordination is not required as it was in the case of public key system. Each device needs just one certificate for key management and one private key that is fixed from the time of installation. However, generating PKI and also having certificate authorities will also have a certain amount of overhead unnecessary for smaller systems.

Elliptic Curve Cryptography. A cryptographic Interoperability strategy (CIS) initiated by National Security Agency (NSA) for government systems selects approved cryptographic techniques. It consists of AES for encryption with 128 or 256 bits. Ephemeral unified model and Diffie-Hell-man key agreement schemes, elliptic curve digital signature algorithm and secure hash algorithm (SHA) for hashing.

5.3. Cryptographic and Key Management Solutions

5.3.1. General Design Considerations

(i) Selection of cryptographic technique should be such that the design is robust and the algorithm is free of flaws.

(ii) Entropy issue can be solved by seeding a deterministic random bit generator (RBG) before distribution or use a key derivation function which comes with the device.

(iii) Use of cryptographic modules that is used to protect the cryptographic algorithm. We need to upgrade these modules timely, since smart grid equipments would be used for around twenty years and also replacing them would be a costlier affair.

(iv) Failure in encryption systems may occur due to implementation errors, compositional failures, insecure algorithms, or insecure protocols. These categories should be taken into consideration while designing.

(v) Since a random number generator is an integral part of the security system, its failures would result in a compromise of cryptographic algorithm or protocol.

(vi) There must be alternatives for authentication and authorization procedures in case we cannot connect to another system.

(vii) Availability must always be there since dropping or refusal to re-establish a connection may affect the critical communication.

(viii) The algorithms and key lengths should be such that the desired security strength is attained.

(ix) In order to maintain security of the keying materials and authentication data, we must protect it from unauthorized access or any device tampering. Physical security is required for this purpose.

5.3.2. Key Management System for Smart Grid. We use certificates that have validity, that is, certificates that have not expired. If this certificate is issued to a device, that is, no longer reliable, either lost or stolen, then the certificate can be revoked. A certificate revocation list is used for this purpose. A device that uses the information in a certificate is called relying party (RP). RP has a checklist that must be considered when accepting a certificate.

The points that need to be checked are as follows

(i) if the certificate was issued by a trusted CA,

(ii) if certificate is still valid and not expired,

(iii) certificate should be in an authoritative CRL,

(iv) verification of the certificate subject and policy for which certificate is being used.

5.4. Approved Algorithms

Symmetric Key. Advanced encryption standards (AESs), triple data encryption algorithm (TDEA), or triple data encryption standard (TDES).

Asymmetric Key. Digital signature standard (DSS), digital signature algorithm (DSA), RSA digital signature algorithm (RSA), elliptic curve digital signature algorithm (ECDSA).

Secure Hash Standard. Secure hash standards (SHSs) and secure hash algorithm (SHA).

Message Authentication. CMAC, CCM, GCM/GMAC (Galois counter mode), and HMAC (hash message authentication code).

Key Management. SP800-108 KDF's.

Deterministic Random Number Generators. FIPS 186–2 APPENDIX 3.1 RNG, FIPS 186–2 APPENDIX 3.2 RNG, ANSI X9.31-1998 APPENDIX A2.4 RNG, ANSI X9.62-1998 ANNEX A.4 RNG, and ANSI X9.31 APPENDIX A.24 RNG using TDES and AES RNG, SP 800-90 RNG.

Nondeterministic Random Number Generators. Currently None.

Symmetric Key Establishment Techniques. FIPS 140–2 1G D.2.

Asymmetric Key Establishment Techniques. SP 800–56 A, SP 800–56 B, and FIPS 140–2 1G D.2.

These algorithms can be studied in detail from [17–34].

6. Privacy

Privacy cannot be defined. The basic definition of privacy would be "the right to be left alone". Privacy should not be confused with confidentiality. Confidentiality of information is information that can be accessed only by a few. In reference to the smart grid privacy means considering the rights, values

and interests of customers (like their personal information, electric signatures, etc.). The data used by smart grid could be used to violate individuals [35].

A privacy impact assessment (PIA) is used for determining the privacy, confidentiality, and secure risks that arise due to the collection, use, and disclosure of personal information. PIA findings and recommendations are as follows [35].

(1) *Management and Accountability*. People should be appointed to ensure that the documented policies for information security and privacy are followed. Audit functions should be present in order to check the data access activity.

(2) *Notice and Purpose.* Before collecting data, using it, or sharing it, a notice must be prepared and exchanged.

(3) *Choice and Consent.* The consumer should be provided with the choices present in context to the energy usage data that could be revealed and their consent should be obtained.

(4) *Collection and Scope*. Only the information that is really necessary should be collected from the user by appropriate lawful means and with their consent.

(5) *Use of Retention.* The information that is collected should be used only for those purposes for what they were taken. Also, the information should be saved in such a way that no activity or information about the consumer can be found out from it. The data should be discarded once its purpose is over.

(6) *Individual Access.* Consumers should be able to see their individual data and can also request for correction if any of the data is inaccurate. They also have the right to know where their information is being shared.

(7) *Disclosure and Limiting Use.* The personal information cannot be shared by anyone not present in the initial notice and should only be used for the reason stated in the notice.

(8) *Security and Safeguards*. The personal information should be secure and must be protected from thefts, modification or unauthorized access.

(9) *Accuracy and Quality.* The personal information should be as accurate as possible and related to the purpose mentioned in the notice.

(10) *Openness, Monitoring, and Challenging Compliance.* A service recipient should be able to access the personal data and should be able to challenge the organizations compliance.

7. Conclusion

The various security concerns related to smart grid was proposed in this paper. Smart grid is an emerging project. Its implementation will result in numerous benefits for the society. However, it has to face a few challenges and concerns when it comes to security. We have studied these challenges in this paper. Cyber security is an integral part of the grids security concern. As the grid develops and expands in the future, the number of nodes that will be not susceptible to cyber attacks will increase. Domain architecture which is used to evaluate these challenges is explained in one of the sections. We then explain cryptography and key management techniques which are used to secure the system against cyber attacks. In this section, we covered the constraints for cryp-tography and also the proposed solutions. The last part of the paper deals with consumer privacy which is another important security parameter that cannot be neglected. In order to make the smart grid more popular, it should be free from any security drawbacks and hazards in order to have a better future.

References

[1] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*, The Fairmont Press, 2009.

[2] "The smart grid: an introduction," http://energy.gov/oe/downloads/smart-grid-introduction-0.

[3] "European smart grids technology platform," http://www.smartgrids.eu/documents/vision.pdf.

[4] F. Li, W. Qiao, H. Sun et al., "Smart transmission grid: vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, Article ID 5535240, pp. 168–177, 2010.

[5] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proceedings of the Power and Energy Society General Meeting (2010 IEEE)*, pp. 1–5, July 2010.

[6] G. Iyer and P. Agrawal, "Smart power grids," in *Proceedings of the 2010 42nd Southeastern Symposium on System Theory (SSST 2010)*, pp. 152–155, March 2010.

[7] Z. Vale, H. Morais, P. Faria, H. Khodr, J. Ferreira, and P. Kadar, "Distributed energy resources management with cyber-physical SCADA in the context of future smart grids," in *Proceedings of the 15th IEEE Mediterranean Electrotechnical Conference (MELECON 2010)*, pp. 431–436, April 2010.

[8] "SCADA," http://en.wikipedia.org/wiki/SCADA.

[9] G. N. Ericsson, "Cyber security and power system communication—essential parts of a smart grid infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, Article ID 5452993, pp. 1501–1507, 2010.

[10] F. Boroomand, A. Fereidunian, M. A. Zamani et al., "Cyber security for smart grid: a human-automation interaction framework," in *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe 2010)*, pp. 1–6, October 2010.

[11] "Cyberspace policy review," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[12] A. Dreher and E. Byres, "Get smart about electrical grid cyber security," http://www.belden.com/pdfs/techpprs/PTD_Cyber SecurityWP.pdf.

[13] "Introduction to NISTR 7628 guidelines for smart grid cyber security," 2010, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.

[14] "Critical electric infrastructure protection act," http://ciip.wordpress.com/2009/04/30/critical-electric-infrastructure-protection-act/.

[15] "The security vulnerabilities of smart grid," 2009, http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96: content&Itemid=345.

[16] "Guidelines for smart grid cyber security vol. 1, smart grid cyber security, architecture and high-level requirements," 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

[17] "Advanced encryption standard (AES)," 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[18] M. Dworkin, "Recommendation for block cipher modes of operation-methods and techniques," 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[19] M. Dworkin, "Recommendation for block cipher modes of operation-the XYS-AES mode for confidentiality on stor-age device," 2010, http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

[20] W. C. Barker, "Recommendation for the triple data encryption algorithm (TDEA) Block Cipher," 2008, http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf.

[21] "Digital signature standards," 2009, http://csrc.nist.gov/publications/fips/fips186-3/fips 186-3.pdf.

[22] "FIPS PUB 186-2," 2000, http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2-change1.pdf.

[23] "Secure hash standard," 2008, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf.

[24] M. Dworkin, "Recommendation for block cipher modes of operation-the CMAC Mode for authentication," 2005, http://csrc.nist.gov/publications/nistpubs/800-38B/SP 800-38B.pdf.

[25] M. Dworkin, "Recommendation for block cipher modes of operation-the CCM mode for authentication and confidentiality," 2004, http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf.

[26] M. Dworkin, "Recommendation for block cipher modes of operation-galois/counter mode (GCM) and GMAC," 2007, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf.

[27] "The keyed hash message authentication code(HMAC)," 2002, http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

[28] L. Chen, "Recommendation for key derivation using pseudorandom functions," 2009, http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf.

[29] "Recommendation guidance for FIPS PUB 140-1 and cryptographic module validation program," 2002, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/FIPS1401IG.pdf.

[30] S. S. Keller, "NIST-recommended random number generator based on ANSI X9.31 appendix A2.4 using the 3 key triple DES and AES algorithms," 2005, http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf.

[31] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generator (revised)," 2007, http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf.

[32] E. Barker, L. Chen, A. Regenscheid, and M. Smid, "Recommendation for Pair wise key establishment schemes using integer factorization cryptography," 2009, http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf.

[33] E. Barker, D. Johnson, and M. Smid, "Recommendation for pair wise key establishment schemes using discrete logarithmic cryptography (revised)," 2007, http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A Revision1 Mar08-2007.pdf.

[34] "Implementation guidance for FIPS PUB 140-2 and the cryptographic module validation," 2010, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

[35] "Guidelines for smart grid cyber security vol. 2, privacy and smart grid," 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.