International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **06** Special Issue **01** | **2021**

Improvement of smart grid stability at times of network attack by using artificial intelligence and block chain

Madhuri Shimpi[1], Prof. S.H.Thakare [2]
[1]*Student, Dept. of Electrical Engineering, PADM.DR.VBKCOE Malkapur, Maharashtra, India.*
[2]*Asst. Professor of Electrical Engineering, PADM.DR.VBKCOE Malkapur, Maharashtra, India.*

ABSTRACT

Renewable energy sources and the increasing interest in green energy have been the driving forces behind many innovations in the energy sector, such as how utility companies interact with their customers and vice versa. The introduction of smart grids is one of these innovations in what is basically a fusion between the traditional energy grid with the IT sector. Even though this new combination brings a plethora of advantages, it also comes with an increase of the attack surface of the energy grid, which becomes susceptible to cyber attacks. In this work, we analyze the emerging cyber security challenges and how the ensuing risks could be alleviated by the advancements in AI and block chain technologies.

Keywords*: *cyber security, block chain, AI, energy grid, smart.

INTRODUCTION

In past decades, the development of power grids has not been keeping pace with industrial and societal advancements that have created an increased demand of power supply. Energy production and consumption increased more than two and three times respectively.1 With this increased demand of electricity, issues like voltage spike and sags, blackouts, and overloads have increased as well, resulting in availability issues which consequently lead to revenue losses for the energy industry. To cope with the aforementioned shortcomings of the energy industry, the need to efficiently manage a variety of energy sources became evident. It also became clear that legacy power systems can no longer meet the requirements of modern society in terms of reliability, scalability, manageability, and cost-effectiveness. These needs gave birth to smart grid, a dynamic and interactive infrastructure with new energy management capabilities, which however inevitably created a system with potential vulnerabilities in terms of cyber security. In this paper, we present some of the most emerging cyber security challenges related to smart grid and discuss mitigation techniques based on block chain and artificial intelligence (AI) Thlocationthe capability both to the provider and to the customer real-time (or near real-time) monitoring of electricity consumption or production, in the case of e.g. photovoltaic cells. They also offer the possibility to read the measurements locally and remotely, and additionally allow the provider to limit or terminate the supply of electricity where appropriate.

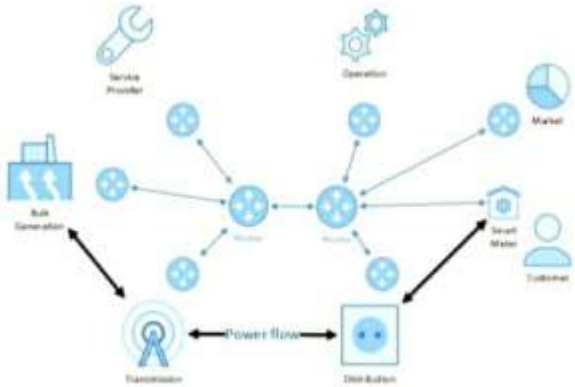

Fig-1: : Network architecture of the Smart Grid.

CYBER SECURITY CHALLENGES

Cyber security poses one of the largest and multifaceted challenges that the smart energy grid and the IoT ecosystem in general will have to address in the years to come. Given the number of interconnected sensors, devices and networks that constitute a smart grid, it becomes evident that it is susceptible to online probing, espionage, and constant exploitation attacks by malicious actors aiming at disrupting the stable and reliable energy grid operation, obtaining sensitive customer information, as well as threatening the CIA triad (confidentiality, integrity and availability) of the network. In order to have a clearer picture of the dangers posed by the integration of smart energy meters in the traditional energy grid, we will examine the security requirements of a smart grid and analyze the most high-profiled challenges from a cyber security perspective.

Cyber security Requirements and Objectives in the Smart Grid

According to NIST, the main criteria required to ensure the security of information in any given information system, thus smart grid as well, are confidentiality, integrity and availability, also known as the CIA triad. It is also widely accepted that accountability is another important aspect of security.

Cyber security Threats and Weaknesses

In this section, we will identify four of the most prevalent cyber security challenges that stem from the integration of IT with traditional energy grid systems.

Cyber attacks

Cyber-attacks on smart grids are a very commonly discussed topic due to the vulnerabilities existing in the grids' communication, networking, and physical entry points. Attacks in the smart grid environment can be categorized into two

• Passive attacks: these are attacks that do not intend to affect system resources and their sole purpose is to extract system information. In these kinds of attacks, the attacker's objective is to learn or use information that it is transmitted, or to retrieve information stored in the system. Generally, passive attacks are relatively hard to detect, since no alteration of data takes place, thus the best defense against them is prevention through solid security mechanisms.

• Active attacks: these attacks are aimed towards a system's resources and attempt to either modify or disrupt them. The most common actors in these kinds of attacks are malicious users, spyware, worms, Trojans, and logic bombs. According to Li et al., the most ordinary types of these attacks are device attacks, data attacks, network availability attacks, and privacy attacks, whereas Wang and Lu classify the attacks as those targeting availability, those targeting integrity, and finally those targeting confidentiality Trust Varying requirements exist for operations performed in smart grids. The system consists of the power grid itself, the communication network, and the devices controlling the process. Honesty and trustworthiness are essential behaviors in the relationship between the consumer and the utility company, thus the validity of the energy bill of the consumed energy is of vital importance from the consumer point of view, whereas the energy provider needs a trustworthy and fully auditable reporting tool for each operating device in the grid. These demands create new challenges that need to be addressed in an environment that all entities cannot be considered as trusted. Therefore, a trusted intermediary entity needs to decide upon the status validity of the devices and manage the access policies for the network, in a way that can authentically report the current state of the network to third parties.

Single Point of Failure

From a reliability perspective, it is well documented that a single point of failure is one of the biggest concerns in a master-slave architecture. In smart grids, a Does attack could disrupt, delay, or prevent the flow of data and eventually even collapse the AMI network. This denial of data exchange means a loss of control messages and may affect the power distribution to the customers in the smart grid. From a scalability perspective, the number of the clients is limited by the capacity of the AMI network in terms of bandwidth and routing capabilities, and the latency is determined by the round-trip time (RTT) between the AMI head end and the devices in the network.

Identity and Access Management

One particular issue with smart meters in smart grids is the management of the cryptographic keys that are required by every meter for cryptographic computations, such as the encryption of the transmitted data. Before the deployment of the AMI, the confidentiality of customer privacy and customer behavior, as well as message authentication for meter reading, and control messages must be ensured. This can be solved by encryption and authentication protocols which depend on the security provided by cryptographic keys. The current industry standard is the use of a X.509 certificate for identification and for establishing a secure connection during data transmission. However, these cryptographic keys remain static for the whole life-cycle of the meter, and a key management mechanism that would allow manufacturers to periodically update or revoke them does not seem to be currently implemented. Furthermore, since such keys are also considered a form of strong device recognition, an attacker could possibly abuse the private key of the device.

Opportunities

The emergence of technologies such as Block chain and Artificial Intelligence (AI)has created a new field for research and innovation, while at the same time offering opportunities in the field of smart energy grids. In the following section, we will attempt to identify some of these opportunities and envision how to apply these technologies in order to countermeasure the aforementioned cyber security challenges.

Block chain Application for Cyber Resiliency:

Block chain is defined as a distributed data base or digital ledger that records transactions of value using a cryptographic signature that is inherently resistant to modification. In a move towards a cyber-resilient energy grid, Block chain could commodities trust and also potentially support auditable multi-party transactions between energy providers and customers. The block chain is the equivalent of a book maintained by a bank, which contains all the accounts and each transaction made. One of the most interesting aspects of block chains is that they contain the records of every transaction made since the beginning, also known as genesis block, by using a peer-to-peer distributed timestamp server which generates computational proof of the chronological order of the transactions. The use of block chain presents numerous potential cyber security benefits to the electricity infrastructure:

Identity of Things:

Identity and access management of the devices in the grid is an issue that needs to be addressed efficiently. The ownership of a device can change during its lifetime or even be revoked in case a consumer is not consistent with his financial obligations towards the energy provider. Apart from ownership, there are also attributes that each device has, such as manufacturer, type, deployment GPS coordinates etc. Block chain is able to address these challenges since it can register and provide identity to connected devices along with a set of attributes that can be stored on the block chain distributed ledger in a fully auditable manner.

• Data integrity: As per block chain's design, every transmitted block in the network, thus all data transmitted by the devices in the grid, are cryptographically signed and proofed by the sender. Each node has its own unique public and private key and thereby it is ensured that the data are encrypted and cannot be tampered. Finally, all blocks are recorded and time stamped on the chain and cannot be changed in a later time, therefore ensuring the accountability and the integrity.

•Securing communications: The most commonly used network communication protocols, such as HTTP, MQTT and XMPP, are not secure by design and thus have to be wrapped within TLS at the application layer. However, protocols such TLS or IPSec rely on complicated and centralized certification authorities for the management of the keys, mainly through a public key infrastructure (PKI). With block chain, there is no longer the need to rely on a centralized authority, since each node in the network receives a Universally Unique Identifier (UUID), as soon as it joins the network, and also creates an asymmetric key pair. This allows to simplify the handshake procedure and use light-weight protocols, such as Tiny TLS, without handling and exchanging PKI certificates during the initial phase of the connection.

AL AND SMART CONTRACTS

Despite the fact that block chain solutions add a layer of cryptography in communications and digital transactions, in complex IoT environments such smart energy grids, many complex cyber security challenges remain. An example is the patch management of the smart meters or their improper configuration. Especially in the first case, the timing between the discovery of a new vulnerability and the deployment of the patch to the affected devices is crucial. In such as scenario, a public repository could be queried periodically in order to check whether a new patch is available. The process could be performed with a block chain-based smart contract, which would validate the transportation of the correct patch and provide an incentive for updating. Such a smart contract could operate on the basis of device-specific information, mainly model and firmware version of the device. According to this data, the contract would decide on whether an update is necessary and instruct the device to perform the update. In case the device is compromised and refuses to update, its trust score could start to decline and the energy provider would be notified regarding the misbehaving device. Whereas the distributed public ledger of block chain may assist in increasing the trustworthiness, AI-enabled smart contracts could add unique value in the timely response to emerging cyber threats like an emergency response to a naturally occurring weather event or a cyber-physical hybrid attack. That way, some functions of the power grid would become self-healing and resilient. Additionally, through the combination of AI and block chain, we could achieve an almost real-time security response to unauthorized attempts to change configurations or network and sensor settings. Anomaly-based intrusion detection systems assisted by Machine Learning (ML), could be an effective method to detect intrusions and attacks, which have not been previously detected. Such a system, combined with the immutability of block chain, could reduce the overhead of the forensics investigation in case of a security incident, by providing a well-established timeline of events for evidence-analysis.

CONCLUSIONS

Smart grid is a system composed of various distributed components with the primary goal to intelligently deliver electricity, while at the same time allows the easy integration of new features and metrics in the traditional grid. Cyber security in the smart grid is a relatively new area of research and in this paper, we presented an initial survey of security requirements and challenges. This was followed by a discussion on opportunities and mitigation techniques based on disruptive technologies such as block chain and AI. Even though the proposed solutions still remain an uncharted territory in smart grid applications, the advancements in block chain and AI make them the more attractive technologies thus far in the pursuit of building a secure and resilient smart grid.

REFERENCES

1. Eric D. Knapp and Raj Samani, Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure (Waltham, MA: Syngress,
2. Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and CL Philip Chen, “Cyber Security and
3. Privacy Issues in Smart Grids,” IEEE Communications Surveys & Tutorials 14, no. 4 (2012): 981-997.
4. Johan Rootzén, “Reducing Carbon Dioxide Emissions from the EU Power and Industry
5. Christopher Greer, David A Wollman, Dean E Prochaska, Paul A Boynton, Jeffrey AMazer, Cuong T. Nguyen, Gerald J FitzPatrick, Thomas L Nelson, Galen H Koepke, and Allen R Hefner Jr., “NIST Framework and Roadmap for Smart Grid Interoperability Standards, release 3.0,” NIST Special Publication, 2014.
6. Fatemeh Halim, Salman Yussof, and Mohd Ezanee Rusli, “Cyber Security Issues in Smart Meter and Their Solutions,” International Journal of Computer Science and Network Security 18, no. 3 (2018): 99-109, http://paper.ijcsns.org/07_book/201803.