Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 07, No. 01, March 2021.

IoT Security for Smart Grid Environment: Issues and Solutions

Yuvaraaj Velayutham, Nur Azaliah Abu Bakar, Noor Hafizah Hassan and Ganthan Narayana Samy

(Received: 27-Jul.-2020, Revised: 10-Oct.-2020, Accepted: 27-Oct.-2020)

Abstract

The Internet of Things (IoT) is the Internet's latest innovation today, where every physical object is situated or where measurement, as well as communication capacities, can be seamlessly synchronized to the Internet at various rates. The most important infrastructure, the smart grid, is called the extended version of the power grid with comprehensive Internet infrastructure. The smart grid will include billions of intelligent appliances: intelligent meters, actuators, vehicles and so on, despite a few correspondence infrastructures, whether public or private. Notwithstanding, security is viewed as one of the primary considerations hampering the large scope reception and arrangement of both the IoT vision and the smart grid. To date, the issues of IoT for the smart grid are rarely discussed empirically in any academic research. This study aims to examine security problems and challenges in the IoT smart grid system. Findings show various issues that we can categorize into three parts; component issues, system issues and network issues. As a result, this study proposes a mitigation plan for the problems highlighted by developing an IoT smart grid security component model.

Keywords

Advanced metering infrastructure, Cybersecurity, Internet of things, Smart grid, Smart meter.

1. Introduction

Internet of Things (IoT) is an emerging domain that evolves from interfacing machines and people to combine smart objects. IoT can be a device that will be an embedded processor or computation device with advanced communications of the machine to machine correspondences [1]. For this intelligence and interconnection, IoT systems include integrated sensors, actuators, processors and transceivers. Sensors and actuators are instruments that support the physical environment. Sensor data must be stored and analyzed intelligently to draw useful inferences from it. An *actuator* is a device that is used to induce a change in the environment. Storage and processing of data can be carried out on the edge of the network itself or in a remote server [2].

IoT devices typically connect to the Internet through the IP (Internet Protocol) stack. IoT devices can also connect locally through non-IP networks which consume less power and connect to the Internet *via* a smart gateway. The leading communication technologies used in the IoT world are IEEE 802.15.4, low-powerWiFi, 6LoWPAN, RFID, NFC, Sigfox, LoraWAN and other proprietary protocols for wireless networks [2]. Nevertheless, some smart devices are still linked to the network through non-IP protocols, such as Bluetooth, RFID and NFC. With the advent of IoT, the smart tool and the protocols, such as IP, TCP or UDP, would be entirely seamlessly related [3]-[4].

The smart grid is an intelligent power system that provides two-way communication back to the database from power generation to electricity distribution to households. A smart grid includes technology applications that promote the incorporation and penetration of renewable energy [5]. It will be necessary to accelerate the production and widespread use of plug-in hybrid electric vehicles (PHEVs) and their potential use as grid storage. Among the benefits of the smart grid are that it is able to provide more reliable power, generate more efficient renewable power and use a mix of energy sources, in addition to being able to work with smart devices and smart homes and most importantly, it will reduce our carbon footprint [6]. Essentially, the smart grid, together with wireless communication-connected smart metres, will monitor how much energy a net-positive enterprise produces and reimburses.

The smart grids form a part of an IoT system that allows all forms of lighting, traffic signals, transport

Y. Velayutham, N. A. A. Bakar, N. H. Hassan and G. N. Samy are with Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia. Emails: yuvaraajvelayutham@icloud.com, azaliah@utm.my, noorhafizah.kl@utm.my and ganthan.kl@utm.my

congestion, parking areas, road warnings and early detection of such items as power inflows due to earthquakes and extreme weather [7]. Wireless devices, such as sensors, radio modules, gateways and routers, are part of the technology that makes the IoT-enabled energy grid "smart". These devices ensure sophisticated connectivity and communication to encourage customers to take more energy use decisions in order to save electricity and expenses in cities and to allow electricity authorities to restore power more quickly after an emergency [5]. The smart grid enables a power provider to analyze system health considerably more fully than before. For example, a power utility can detect real-time demands for power with smart metres with granularity and exactness that is simply not possible with older technology.

Overall, smart grid connectivity networks should comply with time synchronization, reliability, latency and data criticality including support for multicast [8]. Furthermore, interoperability is a big problem in smart grid networking [9]. Most importantly, any device connected to communication systems may be subject to unscrupulous and malicious individuals, whose primary purpose is to access sensitive information [7]. This makes the critical infrastructure to be monitored and operated in a much more efficient manner. This introduces security challenges to the smart grid infrastructure; for example, man-in-the-middle, session hijacking, spoofing and Denial of Service (DOS) attacks [10].

Based on the IoT security issues and challenges arising in a smart grid environment, this paper aims to investigate the existing possible security vulnerabilities. In order to achieve that, this paper will start with a discussion on the use of IoT in the smart grid environment (Section 2), followed by the analysis of security attacks on IoT for smart grid (Section 3). Then, Section 4 will explain the mitigation actions and in Section 5, proposed components for IoT secured smart grid are presented. Finally, in Section 6, the paper concludes with all the related findings.

2. USING IOT IN THE SMART GRID ENVIRONMENT

The future of grid networks is IoT. The National Institute of Standards and Technology (NIST) defined IoT for the smart grid as integrating the old power grid with the current ICT emerging grid [11]. Unlike traditional power grids, the smart grid can sustain or manage power distribution's demand, achieve power delivery efficiency and minimize energy losses [12]. According to the US Department of Energy's Office of Electricity Delivery and Energy Reliability, a smart grid is a digital-infrastructure grid allowing two-way contact between the utility and its customers. The "smart" aspect is its ability to adjust to variable supply and demand. Technologies that yield today's IoT-enabled "smart" energy grid include wireless devices, like sensors, radio modules, gateways and routers [13]. These devices provide advanced networking and communications that encourage customers to make smart choices in terms of energy use, allow cities to conserve resources and costs and enable energy agencies to recover power more quickly after an outage.

2.1 Overview of Smart Grid Design

Smart grid networks are designed to connect various remote controls, smart meters, smart grids, cameras and other network-based products [11]. IoT allows current grid connectivity across the two-way data source and network across the energy system using IoT devices that interconnect customers, distributors and service providers. It can also limit human interference to track meters, home portals and other relevant devices to ensure that grid power is safely managed [14]. Most smart grids follow the NIST defined smart grid model illustrated in Figure 1.

In general, NIST outlines four (4) types of smart grid entity which are: the service provider, the operations, the distribution and the markets. There are three (3) main groups of users; namely, the building or commercial users, the industrial users and home users. Using IoT in the smart grid allows two-way data exchange between the entities and all components of the smart grid [16]. Beside sensors and drives, other intelligent devices and transmitting and storage fields, the touch is conceivable, given the use of smart meters and other smart devices on the end-customer side. This allows the monitoring of energy usage and demand while enabling consumers to watch and change their activities [17].

IoT structures can be guided to another step of efficiency and execution due to a greater degree of controllability and perceptibility, which gives power systems enormous benefits. There are many advantages associated with the smart grid application of IoT. For example, the Advanced Metering

Infrastructure (AMI) can be accessed without any trouble using the IoT smart grid [18]. AMI is responsible for processing, disassembling, storing and distributing the intelligent metering information submitted to the utility organization's billing, outage control and electricity demand forecasting systems. Accessibility of real-time calculation provides consumers and manufacturers with critical signs to better satisfy their energy needs and supplies [11].

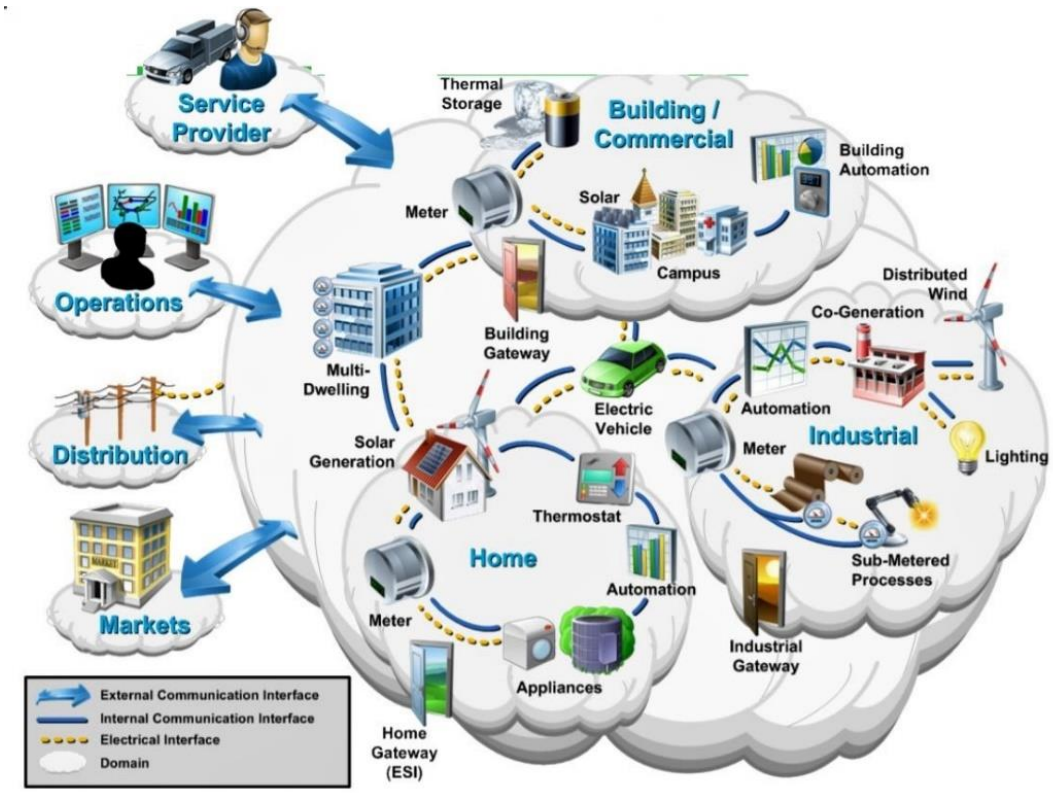

Figure 1. NIST customer domain smart grid model [15].

The IoT smart grid can quickly repair itself (self-recovery) in the event of any external or internal aggravation or risk [18]. It also allows the self-rebuilding of the system, after attacks, cataclysmic events, power outages or breakdown of the network components by complex reconfigurations in order to recover electricity. Besides, it also can create a micro-scale grid and self-sufficiently protected islands in the event of power loss, even as it distinguishes the source of energy leakage [12]. This increases the power grid's performance, modelling and analysis, thereby increasing the power grid's consistency.

Due to the usage of a wide range of sensors, actuators and intelligent meters used to monitor the entire power grid, they may send intermittent data to the utility on-demand or on other occasions while often responding to demands from customers, due to their willingness to communicate in both directions [19]. Added to delivering details on the state of the last mile grid, these instruments can be remotely controlled, managed and operated to include updated Supervisory Control and Data Acquisition (SCADA) features. This helps promote bi-directional electricity, because end-customers can also sell abundant energy from homes, particularly from sources during peak hours, such as sun-based or bio-gas sources around the building [10]. Using the IoT smart grid, this can easily track demand and request reactions on the smart grid, thereby allowing complex electricity pricing components to be influenced. Competitive energy pricing increases peak load management capabilities by charging more significant prices on top occasions to discourage consumption and lower prices at off-peak periods, encouraging reduced utilization and idle use of electricity [14].

The provision of real-time, fast and bi-directional information sharing allows more excellent connectivity with end-users of energy. It provides utilities with a critical insight into consumer consumption habits that further enhance the interconnected grid [11]. The extensive installation of sensors, as well as signal processing and real-time connectivity equipment, helps assess individual grid pieces' position. This helps handle energy, plan for future and current opportunities properly and make

the transmission lines and transformers function in this manner, contributing to a reliable transfer of electricity. These reviews can result in clearly identifying signs of line defects, a decrease in the risk of catastrophic failure and a decline in operation and repair costs in these lines, thereby improving the unwavering efficiency of the transmission system [8].

2.2 The Benefits of Smart Grid

Today, the current grid faces challenges daily; for example, blackouts, current overloading and service disruption in a particular area. However, this is only determined if the end-user files a complaint on the occurrence. In contrast, with the implementation of smart monitoring on the grid, we can react proactively to the downtimes. Smart grid technology is the key to easy integration and customer reliability [8]. This system can solve problems very quickly in a current system since it can reduce the workforce and strive for sustainable, effective, secure and quality energy for all consumers. According to [13], [20]-[22], the following are the benefits of smart grid technology.

Smarter Energy Use: The technology from smart grid helps reduce energy usage and costs by using and retaining data. Smart lighting, for example, can be tracked around various areas by using smart urban technology, immediately accommodating settings like rain, changing the production to suit traffic conditions or time of the day and instantly identifying light outages and fixing them. Users can change the temperature of their home thermostats for use in consumer applications when working or on holiday [21].

Cleaner Energy Use: Smart grid technologies have lower battery requirements, are carbon-efficient and are designed to reduce the maximum load of distribution feeders. The US Department of Energy is incorporating renewable technologies into its intelligent IoT management framework for sustainable solutions. There is an ability to support all levels of the distribution network through integrated wind turbines, solar panels, micro-grid technologies and feeder automation systems [13].

Lower Costs: Today, power outages and interruptions of the electricity system cost Americans at least $150 billion per year and set the price tag of about $500 per person. If the world's population continues to expand, the older networks cannot meet growing demands. Smart grids are built to reduce costs by monitoring intelligent electricity and redirecting the source from the moment a power failure is detected [13].

Improved Transportation and Parking: IoT smart sensors can collect data in real-time for drivers and authorities to obtain information. Ultimately, this would reduce traffic delays, provide better parking options, alert drivers to traffic events and townscape structural damage and allow electronic payment at road tolls and car park metres. Future IoT technology is also expected to charge electric vehicles wirelessly [20].

Assistance in Waste and Water Management: The smart network will benefit smart cities by rising their productivity and reducing their waste management solution costs. In order to track inventory and minimize fraud, IoT apps can provide real-time data. Cloud-based monitoring and traffic management can increase time and scheduling on lorry routes. Smart energy analytics can collect data about water flow, pressure, temperature and much more, which allows customers to keep track of their usage practises [21].

Energy Enablement in Developing Countries: Smart grids could be used to convert power to sparsely populated regions from simple on-off electrification methods; for example, from battery-based household electrification to neighbourhood grids, which would then connect to national and regional grids. These grids would be crucial for the implementation of new energy infrastructures in developing countries that are suffering from the consequences of the overflowing population. This will potentially pave the way for economic development [22].

IoT allows the remote detection and control of smart grid resources through an adaptable communication network that enables better synchronization between the physical environment and PC-based control systems [12]. This is proven to improve productivity and precision and allow the grid to meet present-day and future energy needs. However, the advancement of technologies always comes with challenges, especially in terms of security. The following section will discuss the IoT security issues in the smart grid area.

3. Related Works on IoT for Smart Grid Security Issues

In the literature, the need for detailed investigation of smart grid security issues has been suggested [9]-[10], [17]. The energy industry is essential, and without doubt, cybersecurity challenges will be present and faced by smart grid IoT devices. IoT devices on a grid environment may reach hundreds and thousands of tools spanning across the regions; they are most vulnerable to cyberattacks. Malware threat is a significant hindrance to efficient information exchange on the IoT [23]. A cyber-attack on these IoT devices may cause loss of valuable data or even halt in company production. For example, in 2015, an attack on the Ukrainian power grid made it possible for hackers to stop and monitor the network with BlackEnergy malware in order to hack the grid and SCADA Network. This resulted in a vast blackout, where over 700,000 users did not receive any electricity [24]. This clearly showed that security is a significant impediment to the introduction or service of the IoT-based smart grid.

What makes IoT protection more complicated is the big number of tools deployed which would not add security to the devices. Unlike computers, we would be able to reinstall or wipe the entire network, but most IoT devices do not support that just yet. A study by Salameh, Dhainat and Benkhelifa [25] showed that the efficiency of these wireless network sensor systems varies as many IoT devices are mostly tied to the manufacturers. The end consumers do not have access to fiddle with the devices as the manufacturers lock them [26]. This paper presents IoT security issues in the smart grid distributed over three classifications; firstly the component security issues, secondly the system security issues and thirdly the network security issues.

3.1 Issues of Component Security

Many experts and engineers have evaluated the safety deficiency of the smart meter. A malicious code attack may disrupt the expected behaviour of the intelligent meter. DOS attacks can be powered to avoid the contact of legitimate smart meters with different nodes. For example, an unapproved node can perform eavesdropping (passive man-in-the-middle) stealthily to identify sensitive data about the client's energy use, current charges and appliances used in the household [8]. Furthermore, an attacker can send out false information imitating to be the legitimate smart meter. There is a function in smart meters called Remote-Connect-Disconnect. This function enables operators or engineers to collect the maintenance information from the meter for troubleshooting purposes. This allows a back door in the smart meter itself for the attacker, and the attacker may use this to falsify the data of the meters [17].

The IoT smart grid network has been named a home portal, which receives information from the smart meter on power usage and shows it on the household's mobile device or even the computer. The home app or smart meter provides a service provider with power usage information for budgetary benefit. However, eavesdropping will destroy this gateway communication [17]. Another threat is posed by the Phasor Measurement Unit (PMU) device, which can gather field estimations sending voltages and electrical quantities to the Phasor Data Connector (PDC). The PDC perceives the information from various PMUs, mixes it as a single post.

Moreover, it interacts with other operating domains. A malicious node can spoof PMU attacks, alter PMU messages, provide estimated vitality data and even replay PDC and PMU messages. Such attacks impact critical decision-making processes, such as fault detection and location of incidents. For instance, when an attacker replays an old PMU message that contains vitality estimation misfortunes or line blackouts, the operating system may choose to kill the power for a zone [14].

3.2 Issues of System Security

Smart grid operations have a few control frames which with similar goals and specifications. The Energy Management System (EMS) and the Delivery Management System (DMS) will assume transmission control and energy dispersal. At the same time, SCADA will assist in electronic power systems [5]. Hence, such control and management systems that conduct critical tasks, such as regulating voltage, identifying blackouts, transferring power intensity for distribution and transmission of electricity, should be protected from attacks. They are vulnerable to malicious node attacks that target the DoS control systems, which will later affect their functionality.

Similarly, a false information attack against a control system will influence the smart grid automated decisions. For instance, sending invalid measure energy will affect the distribution and transmission

activities. At the same time, systems depend on false PMU data control choices. A malicious node can replay PMU transmission estimation information; thus, the control centre concludes the decision based on the PMU data [27]-[28]. Messages are transmitted in multi-hop within the AMI system and interchanges between smart meters and the control centre. Therefore, it is possible to accelerate man-in-the-middle attacks and change the energy consumption data before transmitting messages. Moreover, there is a possibility for an attacker to stealth-listening on data trading between the smart meter and the control centre through a remote communication channel.

The Wide Area Monitoring Protection and Control System (WAMPAC) will share information on transmission with other control systems, delivering real-time monitoring and warning capability and maintaining effective transmission and aggregation of electric grids. The grouping of attacks indicates that the WAMPAC system is additionally vulnerable to Denial-of-Service (DOS) attack. At the same time, applications give real-time activity and performance [27]. DOS attacks can occur in different layers of communication. For example, a malicious node can transmit jamming that fills the small-medium with noise flags and can severely impact the data in real-time [28]. The jamming attack will harm the system's functionality, and an authentic node cannot get messages back. Besides, different kinds of assaults; for example, spoofing and man-in-the-middle, can be pushed only as the full or partial channels of communication can be jammed. One more aspect to be considered is the malware attack. Malware threat is a significant hindrance to efficient information exchange on the IoT, including for the smart grid [23]. Modelling malware propagation is one of the most imperative applications aimed at understanding the mechanisms for protecting the smart grid environment.

3.3 Issues of Network Security

The Neighborhood Area Network (NAN) protects and tracks smart meter connections in a single geographical area. Conventions that are available on NAN systems include the Routing Protocol for Low Power and Lossy Networks (RPL), the Minimum Transmission Energy Protocol (MTE) and the *Ad Hoc* on Demand Multipath Distance Vector (AOMDV) [15]. The smart grid network's basic features can be targeted under various attacks by the RPL routing protocol for NAN networks. For example, the Wireless Sensor Network (WSN) attacks will affect the IoT RPL directing convention. WSN is a group of spatially deployed sensor nodes that acknowledge or remotely observe diverse environmental variables or natural events. The sensor nodes are used to collect the surrounding natural events, process data, respond to base station requests and commands or transmit the data to other neighbour sensors. These features indirectly expose WSN to more types of attacks, including DoS attack due to the open wireless communication and physical risks [29]. Currently, the Home Area Network (HAN) can handle the link between the smart meter and the HAN devices. HAN can use distinctive networking technologies, such as Zigbee, Bluetooth and WiFi [3]. Present protection protocols, such as IDS, IPsec, VPN and PKI, can be extended to the smart grid; however, it is still inadequate to guarantee that these protocols are secured for the smart grid environment.

In summary, we conclude the possible attack types and their classification associated with the Smart Grid IoT implementation in Table 1.

Table 1. IoT smart grid possible security issue and attack types.

Security Issue Classification	Attacked Type	Related Study
Component Security	• Malicious code attack • DOS attacks • Passive man-in-the-middle • False information from smart meter • Phasor Measurement Unit (PMU) attack • Phasor Data Connector (PDC) attack	[8], [14], [17]
System Security	• Energy Management System (EMS) attack • Delivery Management System (DMS) attack • False information attack • Man-in-the-middle attacks • Stealth-listening • WAMPAC system attack	[5], [23], [27], [28]

	• DOS attack • Malware threat	
Network Security	• Routing Protocol attack • Wireless Sensor Network (WSN) attack • DoS attack	[3],[15], [29]

Until now, the concept of IoT has concentrated on the demand side, with little attention to the supply side. Smart grid technologies all contribute to efficient IoT energy management solutions that are currently lacking in the existing security framework. The next section explains the mitigation control for the security concerns highlighted.

4. MITIGATION OF SECURITY CONCERNS

With the current emerging technology and fast-evolving internet technologies, IoT devices are an essential element in the network. However, with the implementation of IoT with the smart grid, it should be further secured and guarded at all times. From the previous discussion on smart grid security issues, this paper highlighted a few components that could be implemented to prepare the environment to face the attacks over the smart grid network.

Firstly, a guideline must be established to ensure the rules and regulations of IoT in a smart grid environment. This includes access to grants and privileges. Getting these predefined access privileges to grid devices and network functionality eliminates the possibility of malicious user access [30]. The IoT-based smart grid is a centrally managed and optimized cyber-physical system; access controls are necessary to ensure network connectivity to customers and devices. For example, in access control aspects, Discretionary Access Control (DAC), Compulsory Access Control (MAC) and Roll-based Access Control (RBAC) will extend unwavering consistency and dispense with possible safety hazards.

While deploying IoT systems, traffic between IoT devices and control centres, including utility-supported servers, needs to be encrypted. As mentioned by [1], encoding messages using rigorous encryption methods is crucial, because it diminishes an intruder's ability to decrypt data or produce useful information for trickery. It ensures both material security and secrecy, as it involves identifying computers in the system and authorizing what each network machine completes. System authentication is typically the central stage of software exchange sessions, often culminating in a shared session key for encryption and verification of data packets and maintaining performance validity [31]. Since IoT smart grid contact is time-sensitive and traffic-intensive, an authentication scheme will need little messaging interaction between grid devices. The authentication process will ensure that the meter will not accept commands from an unapproved system. In contrast, the validation process will provide identity verification and acceptance.

IoT systems must be scalable to be upgraded to implement bugs and software upgrades fairly and effectively [32]. Unfortunately, most developers now develop software without contemplating applying any leap of imagination to update potential firmware [33]. Nonetheless, they will accept that creativity, operating systems and computer code look at potential threats and flaws in the future and improvements will be made to address these problems. Deploying firmware upgrades can be difficult if not designed to provide upgrades. Given a smart IoT system's sheer size, frequent firmware overhaul upgrades are the sensible and rational approach relative to the significant replacement of outdated systems in reach. Cybersecurity concerns are significantly heightened when businesses mix modern and old technologies, irrespective of overall network security. Consequently, maintaining a steady protocol that considers agile software delivery would cause the network security vulnerability to be closed, thus mitigating possible hazards.

The environmental stability of all grid systems is paramount. The tamper-resistant device can be used and integrated into grid segments to avoid unwanted physical entry. Remote exposure by unauthorized workers will lead to data stored, such as authorization, identity, use and account details in compromised computers [8]. Remote wiping technologies should be set up to uninstall or lock network resources to protect confidential private information from leaking because intruders can use them maliciously. It is crucial to strengthen the physical security of the facilities, where servers and control rooms are located [34]. This provides a focus area from which those intending to damage the network, such as hackers and disgruntled former staff, can easily control the entire IoT smart grid.

While designing IoT for smart grid applications, integrity and end security will remain the critical factor, since the IoT devices may be used for surveillance or law enforcement purposes. Nevertheless, it also can be exposed as a double-edged weapon, whereby it can be exploited by a terrorist [10]. Therefore, from the beginning, both manufacturers and users should ensure that no bypass or malicious code is installed on the smart grid application. They should also ensure that they do not mass-produce devices with a single arrangement of default logins and should not render specific logins for each model, because this provides an easy opportunity for DoS attacks on the devices.

DoS attacks are the IoT's most crucial challenge. Thus, a viable network layer programming approach is required to prevent DoS assaults [35]. This can be resolved by using the fast hopping Internet Protocol (IP). It allows consumers an easy way to cover their contact sessions' content and destination site. This is achieved by concealing a server's real IP address behind a large pool of IP, which ultimately impedes the detection of network traffic destination through various switches. The real-time shift in the server's IP address happens concurrently with all registered customers and applications.

5. PROPOSED COMPONENTS TO SECURE SMART GRID WITH IOT

From the discussion on the IoT smart grid security issues and the suggested mitigation control, this study proposes an IoT Smart Grid Security Strengthening model. This model focuses explicitly on strengthening because we believe that the initial security aspect has been implemented in both IoT and smart grid design. However, due to unexpected cybersecurity threat, specifically on IoT, the additional model will be beneficial to ensure security adherence. Figure 2 shows the proposed model discussed.

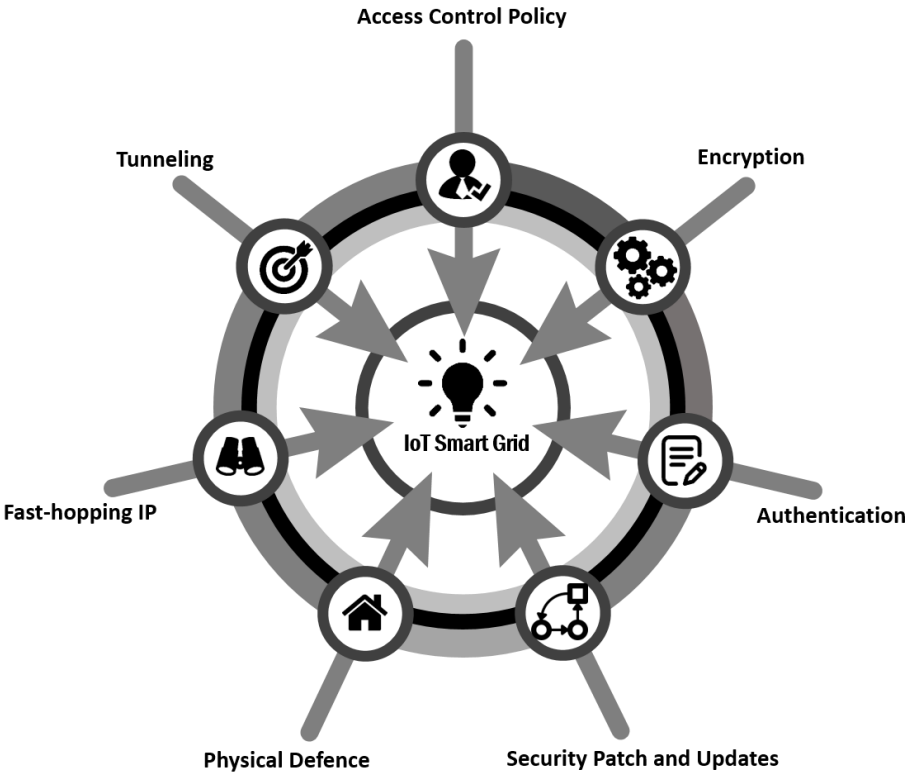

Figure 2. IoT smart grid security strengthening model.

There should be an ***access control policy*** in place in the environment. In that manner, we can avoid intruders from gaining physical or logical access to the critical infrastructure, besides encryption. As dangerous as the IoT network could get, state-of-the-art ***encryption*** on the communication is essential. For example, we could use MD5 or SHA 256 or 3DES to encrypt the data that is being stored. Password and credential policy plays a vital role. There must be an ***authentication*** mechanism in place for the systems to recognize and identify legitimate users. The authentication mechanism will then block intruders. This will not make it an easy process for intruders to get into the system. There must not be a natural or common password being used.

As soon as the ***security patch and updates*** are installed, they should be considered to be updated on the smart meter or IoT devices. Improper test on the security updates and pieces may break the existing equipment. It is highly suggested to test the development environment before implementing the production environment, which indirectly allows the closure of backdoors and loopholes in the system. Furthermore, there must not be a single loophole or backdoor in the critical infrastructure. The fundamental issue to consider is ***physical defence***. As we learn, smart grid SCADA and IoT are the most vital technologies. Environmental protection is essential and can be used as first-level security for an organization against intruders and natural disasters. ***Fast-hopping IP*** implements an innovative Internet security solution which should not be neglected. Thus, the network does not use static TCP, which helps protect the system and delay the attacker attempt. ***Tunnelling*** will be built to protect this vital infrastructure further; for example, the IPSEC tunnel or site-to-site tube. It will cover the smart grid network from man-in-the-middle-attacks and any other similar attacks.

Smart electronic devices need end-to-network systems worldwide to protect the smart grid from the control centre to the broadcast substations. This technology includes network-level monitoring systems, such as Home Access Network (HAN), Neighbourhood Access Network (NAN) and Family Access Network (FAN), with endpoint devices, such as smart meters or other Intelligent Electronic Devices (IEDs), substations and control centres. A smart grid access system allows for numerous networking advancements, such as Zigbee, Wimax and WI-Fi.

For example, HAN addresses specific mobile gadgets using the Zigbee protocol. Within a Zigbee configuration, Particular Zigbee provides different machine security arrangements. Contemplating introducing Zigbee security modules to handle Zigbee technology remains a flexible research point within the HAN. However, Zigbee specifications are meant for simplified activities, such as remote controls. Zigbee's partnership functions to make the NAN mesh network a standard. The network field can establish Wimax-dependent connectivity between remote devices and substations. Thus, configuring the similar networking systems used in the smart grid will ensure that the smart grid network works to the end of the security infrastructure.

Furthermore, the use of IPsec convention needs a commitment to incorporate an end-to-end smart grid security network. This case involves an IPsec investigation into Zigbee and Wimax. Zigbee has been designed for local networks, so web-based apps do not talk explicitly. Not just that; specifically, HAN and smart meters require Internet data transmission. The 6LowPAN allows sharing IPv6 packets to and from IEEE802.15.4-based systems. If 6LowPAN is used in the home area network, expanded security prerequisites must be addressed. Additionally, Wimax's IP-based protection for the FAN network must be investigated as an IPsec's configuration in the smart grid network, which may pose several problems because it has different specifications.

6. CONCLUSION AND FUTURE WORK

In this paper, we highlighted that securing the smart grid network is essential, as the data exchanged is sensitive, and the management operations are crucial. The smart grid is spread out in various spaces, as heterogeneous devices and systems are used in a distributed manner. We categorized types issues of security; firstly component security, secondly system security and thirdly network security. For component security, the smart meter is a vital element which is vulnerable to various forms of assaults, such as spoofing, eavesdropping, infusing false information and targeting replays. We have also featured that an intruder can spoof the smart meter's character to gain access to all home devices.

For system security and network security, DOS attacks are the frequent attack type that can influence control systems rendering devices inaccessible to network demands. Besides, there is also the man-in-the-middle attack on the AMI network and unique sending assault on conventions that separate an excellent hub that does not have the option to reach its neighbours and the control location. Therefore, this paper highlighted the essentiality in implementing an end-to-end security engineering, access control, physical security, frequent patches and updates, fast hopping IP and tunnelling to protect the smart grid.

The proposed model has the potential to identify threats accurately and can provide an extensive security measure when supplied with adequate IoT smart grid equipment. At this moment, this proposed model is still at the experimental scope, and it still requires much experimentation to distinguish an optimal

parameter with the real IoT smart grid evaluation. The IoT is capable of changing how we think of cities around the world. In order to improve and replace old architectures, IoT links people and governments to innovative urban solutions by inventing smart grid technologies. Corporations, utilities and private citizens that use grid power and thus benefit from the implementation of smart grid technologies by municipalities include all residents, urban services and critical infrastructures. The intelligent grid is stable, effective, green and good for customers, utility companies and the environment.

ACKNOWLEDGEMENTS

The authors thank the distinguished reviewers for reviewing this article. The research is financially supported by Universiti Teknologi Malaysia (UTM) Transdisciplinary Research (TDR) Grant Q.K130000.3556.06G26.

REFERENCES

[1] K. Kandasamy, S. Srinivas, K. Achuthan and V. P. Rangan, "IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors and Risk Ranking Process," EURASIP Journal on Information Security, vol. 2020, pp. 1-18, 2020.

[2] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols and Applications," Journal of Electrical and Computer Engineering, vol. 2017, pp. 1-25, 2017.

[3] B. Champaty, S. K. Nayak, G. Thakur, B. Mohapatra, D. Tibarewala and K. Pal, "Development of Bluetooth, Xbee and Wi-Fi-based Wireless Control Systems for Controlling Electric-Powered Robotic Vehicle Wheelchair Prototype," Robotic Systems: Concepts, Methodologies, Tools and Applications, IGI Global, pp. 1048-1079, 2020.

[4] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats and Solution Architectures," IEEE Access, vol. 7, pp. 82721-82743, 2019.

[5] S. K. Rathor and D. Saxena, "Energy Management System for Smart Grid: An Overview and Key Issues," International Journal of Energy Research, vol. 44, no. 6, pp. 4067-4109, 2020.

[6] X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid—The New and Improved Power Grid: A Survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, 2011.

[7] S. K. Goudos, P. Sarigiannidis, P. I. Dallas and S. Kyriazakos, "Communication Protocols for the IoT-based Smart Grid," IoT for Smart Grids, pp. 55-83, Springer, 2019.

[8] F. Dalipi and S. Y. Yayilgan, "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges," Proc. of the 4th IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 63-68, Vienna, Austria, 2016.

[9] B. Jelacic, I. Lendak, S. Stoja, M. Stanojevic and D. Rosic, "Security Risk Assessment-based Cloud Migration Methodology for Smart Grid OT Services," Acta Polytechnica Hungarica, vol. 17, no. 5, pp. 113-134, 2020.

[10] M. Z. Gunduz and R. Das, "Cyber-security on the Smart Grid: Threats and Potential Solutions," Computer Networks, vol. 169, p. 107094, 2020.

[11] L. Tightiz and H. Yang, "A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication," Energies, vol. 13, no. 11, p. 2762, 2020.

[12] A. Ghasempour, "Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies and Challenges," Inventions, vol. 4, no. 1, p. 22, 2019.

[13] M. Faheem *et al.*, "Smart Grid Communication and Information Technologies in the Perspective of Industry 4.0: Opportunities and challenges," Computer Science Review, vol. 30, pp. 1-30, 2018.

[14] S. Eom and J.-H. Huh, "The Opening Capability for Security against Privacy Infringements in the Smart Grid Environment," Mathematics, vol. 6, no. 10, p. 202, 2018.

[15] S. Lee, H. Lim, W. Go, H. Park and T. Shon, "Logical Architecture of HAN-centric Smartgrid Model," Proc. of the IEEE Int. Conf. on Platform Technology and Service, 2015, pp. 41-42, Jeju, S. Korea, 2015.

[16] T. Alladi, V. Chamola and S. Zeadally, "Industrial Control Systems: Cyberattack Trends and Countermeasures," Computer Communications, vol. 155, pp.1-8, 2020.

[17] K. Kimani, V. Oduol and K. Langat, "Cybersecurity Challenges for IoT-based Smart Grid Networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36-49, 2019.

[18] A. Ghosal and M. Conti, "Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey," IEEE Communications, Surveys & Tutorials, vol. 21, no. 3, pp. 2831-2848, 2019.

[19] T. Alladi, V. Chamola, J. J. Rodrigues and S. A. Kozlov, "Blockchain in Smart Grids: A Review on Different Use Cases," Sensors, vol. 19, no. 22, p. 4862, 2019.

[20] G. Dileep, "A Survey on Smart Grid Technologies and Applications," Renewable Energy, vol. 146, pp. 2589-2625, 2020.

[21] N. S. Nafi, K. Ahmed, M. A. Gregory and M. Datta, "A Survey of Smart Grid Architectures, Applications, Benefits and Standardization," Journal of Network and Computer Applications, vol. 76, pp. 23-36, 2016.

[22] N. Nidhi, D. Prasad and V. Nath, "Different Aspects of Smart Grid: An Overview," Nanoelectronics,

Circuits and Communication Systems, Part of the Lecture Notes in Electrical Engineering, vol. 511, pp. 451-456, Springer, 2019.

[23] K. E. Mwangi, S. Masupe and J. Mandu, "Modelling Malware Propagation on the Internet of Things Using an Agent-based Approach on Complex Networks," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 6, no. 01, pp. 26-40, 2020.

[24] J. E. Sullivan and D. Kamensky, "How Cyber-attacks in Ukraine Show the Vulnerability of the US Power Grid," The Electricity Journal, vol. 30, no. 3, pp. 30-35, 2017.

[25] H. B. Salameh, M. Dhainat and E. Benkhelifa, "A Survey on Wireless Sensor Network-based IoT Designs for Gas Leakage Detection and Fire-fighting Applications," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 5, no. 02, pp. 60-72, 2019.

[26] E. Manavalan and K. Jayakrishna, "A Review of Internet of Things (IoT) Embedded Sustainable Supply Chain for Industry 4.0 Requirements," Computers & Industrial Engineering, vol. 127, pp. 925-953, 2019.

[27] P. A. Pegoraro, A. Meloni, L. Atzori, P. Castello and S. Sulis, "PMU-based Distribution System State Estimation with Adaptive Accuracy Exploiting Local Decision Metrics and IoT Paradigm," IEEE Transactions on Instrumentation and Measurement, vol. 66, no. 4, pp. 704-714, 2017.

[28] A. Meloni, P. A. Pegoraro, L. Atzori and S. Sulis, "An IoT Architecture for Wide-area Measurement Systems: A Virtualised PMU-based Approach," Proc. of the IEEE International Energy Conference (ENERGYCON), pp. 1-6, Leuven, Belgium, 2016.

[29] I. Almomani and K. Sundus, "The Impact of Mobility Models on the Performance of Authentication Services in Wireless Sensor Networks," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 06, no. 1, pp. 75-93, 2020.

[30] N. A. Bakar, W. M. W. Ramli and N. H. Hassan, "The Internet of Things in Healthcare: An Overview, Challenges and Model Plan for Security Risks Management Process," Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 15, no. 1, pp. 414-420, 2019.

[31] N. Židková, M. Maryška, P. Doucek and L. Nedomova, "Security of Wi-Fi As a Key Factor for IoT," Hradec Economic Days, DOI: 10.36689/uhk/hed/2020-01-101, 2020.

[32] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama and J. Shah, "IoT Security Risk Management Model for Healthcare Industry," Malaysian J. of Comp. Science, vol. sp2019, no. 3.9, pp. 131-144, 2019.

[33] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures," Proc. of the 10th IEEE International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336-341, London, UK, 2015.

[34] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," Proc. of the 1st IEEE International Workshops on Foundations and Applications of Self* Systems (FAS* W), pp. 242-247, Augsburg, Germany, 2016.

[35] T. Alladi, V. Chamola, B. Sikdar and K.-K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 2020.

"IoT Security for Smart Grid Environment: Issues and Solutions," Y. Velayutham, N. A. A. Bakar, N. H. Hassan and G. N. Samy.

ملخص البحث:

تعدّ إنترنت الأشياء آخر إبداعات الإنترنت هذه الأيام، وتعد البنية التحتية الأهم - الشبكة الذكية- النسخة الموسعة من شبكة القدرة، وهي ذات بنية إنترنت شاملة. وتحتوي الشبكة الذكية على بلايين الأجهزة الذكية؛ كالمقاييس الذكية، والمشغلات، والنواقل وغيرها، مع وجود القليل من البنى التحتية الخاصة بالتراسل.

وتجدر الإشارة الى أن الأمان ينظر اليه على أنه الشاغل الأبرز الذي يعيق الاستقبال واسع النطاق والترتيب المتعلق برؤية كلٍ من إنترنت الأشياء والشبكة الذكية.

ترمي هذه الورقة الى فحص المشكلات والتحديات المرتبطة بالأمان في أنظمة إنترنت الأشياء - الشبكة الذكية. وقد أسفرت الدراسة عن مسائل متعددة يمكننا تصنيفها في ثلاث فئات: مسائل متعلقة بالمكونات، وأخرى متعلقة بالأنظمة، وثالثة متعلقة بالشبكة. وبناءً على ذلك، يقترح الباحثون خطةً للتخفيف من المشكلات الخاضعة للدراسة؛ عبر تصميم أنموذجٍ للحفاظ على أمان انظمة إنترنت الأشياء - الشبكة الذكية.