ECS PMA

Student ID or IDs for group work	2126529
Words	3087

Date set	19th May 2023
Submission date (excluding extensions)	19/06/2023 by 12:00pm (UK time)
Submission guidance	To be submitted electronically via Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	Enterprise Cyber Security (ECS-WM088-15, CSE)
Module owner	Elzbieta Titis
Module tutor	Peter Vincent
Module marker	Elzbieta Titis
Assessment type	Report
Weighting of mark	100%

1. Executive Summary

This report provides readers with an introduction to the smart grid, including its concepts, limitations, as well as the discussion of innovative research and solutions proposed in relevant literature. In addition, we will discusse the layered model of cloud-based information infrastructure and compared it with the centralised model to provide readers with an understanding of the differences between different models. Furthermore, we will provide the cybersecurity issues of the cloud-based information infrastructure and highlighted the necessity of cybersecurity for organisations. Finally, we will conclude the report and discussed examples of challenges faced by the cloud-based information infrastructure, offering readers an insight into the limitations that come along with the convenience of the cloud.

2. Introduction

In this section, we will discuss the concept of smart grid, the role of cybersecurity in smart grid and the current limitations of information infrastructure. Moreover, we will provide high-quality academic research papers concerning the identity issues of endpoints and users in smart grid, and delve into their significance and reflections.

2.1 Conception of Smart Grid

The smart grid is a new generation of self-sufficient power network that integrates information technology, advanced communication technologies, and power systems to realise the modernisation and intelligence of the power network. The aim of the smart grid is to enhance the reliability, security, economic efficiency, and sustainability of the power system through automation and high levels of interaction, while reducing the need for manual labour (Colak, 2016)[1].

Key components of the smart grid include smart appliances, smart metering devices, smart grid transmission networks, and distributed generation and storage devices. With these components, the smart grid is not only capable of collecting, monitoring, and optimising power data, but it can also effectively facilitate two-way data and information transmission between users and the energy system.

2.2 Cybersecurity Role in Smart Grid

Given that the operation of endpoints within the smart grid is heavily reliant on the internet, such as device data monitoring and optimisation, remote control and adjustment by operators, and system

[1] Colak, I. (2016) Introduction to smart grid. [online] Available at: https://ieeexplore.ieee.org/document/7548265

security and troubleshooting, cybersecurity is critically important to the smart grid. In the following, we list three essential roles of cybersecurity in the smart grid:

Device security and operational protection: Most devices in the smart grid are network-connected. If devices are not properly protected and are thus subjected to cyber attacks, it could result in device damage and lead to economic losses, or even threaten the normal functioning of society.

Data security and privacy protection: The control centre in the smart grid collects a vast amount of data from devices and users. We could ensure data security through the effective implementation of cybersecurity measures, thereby safeguarding system data and users' privacy.

Identity verification and access control: The smart grid contains numerous endpoints, including many grid devices, personnel, and users. We could prevent unauthorised access by conducting identity verification and access control on various endpoints within the smart grid.

2.3 Address Limitations of Current Information Infrastructure for Future Grid

With the advancement of technology, we are seeing an increasing number of cloud-based hardware and systems being used in smart grid to handle vast amounts of data. However, despite the many advantages that cloud technology brings to data processing and storage in power grid, there are some unavoidable limitations. In the following, we present several limitations and corresponding solutions of current information infrastructure for future grid:

Network stability: Network stability of smart grid could be compromised by issues with providers, equipment failures, or adverse weather conditions, causing delays or disconnections. Therefore, we could address this issue using edge computing or backup systems.

Data security and privacy: Data uploaded to the cloud could potentially be compromised or misused by attackers. Thus, we could employ data protection policies and secure encryption technologies to protect data in the cloud.

Identity verification and access control: A cloud-based smart grid may involve thousands of endpoints connecting to the cloud, necessitating extensive management. Thus, we could establish a unified identity management system and access control list to protect endpoints and users.

Flexibility: Due to an increasing number of devices and systems will quickly connect to the smart grid in the future, cloud services need to be scalable to rapidly adapt to current demands. Therefore, we need to work closely with cloud service providers to establish efficient processes for monitoring the grid and adjusting resources in real time.

Legal regulations: Different countries and industries have different regulations for data, which may limit the ways in which cloud service data is processed and used. For example, the General Data Protection Regulation (GDPR) in Europe stipulates how businesses and organisations handle personal data. Thus, we could collaborate with legal experts and service providers to ensure compliance with legal regulations.

2.4 Related Works

In this part, we will present relevant high-quality academic research papers in smart grid and engage in reflection. The research papers include solutions proposed for threats brought about by communication transmission and data sharing environments within smart grid. In the reflection, we will discuss and provide insights into the issues of endpoints and user identity within smart grid.

2.4.1 Securing Demand Response Management: A Certificate-Based Access Control in Smart Grid Edge Computing Infrastructure (Chaudhry et al., 2020)[2]

This research proposes a novel Demand Response Management Authentication Scheme (DRMAS) that addresses the security threats brought about by frequent data transfers in a smart grid environment. The new scheme covers all necessary security requirements and has the capacity to counter known attacks. Furthermore, the authors mention that DRMAS only requires two message exchanges and completes the authentication process in a very short time (only 20.11 milliseconds), demonstrating its efficiency (Chaudhry et al., 2020)[2].

2.4.2 Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks (Gai et al., 2019)[3]

This research introduces a new model for smart grid networks, dubbed PBEM-SGN, which integrates blockchain and edge computing technologies to provide flexible communication services and address privacy and security issues within the smart grid. This innovative approach uses unique signature and

[2] Chaudhry, S.A., Alhakami, H., Baz, A. and Al-Turjman, F. (2020). Securing Demand Response Management: A Certificate-Based Access Control in Smart Grid Edge Computing Infrastructure. *IEEE Access*, 8, pp.101235–101243. doi:https://doi.org/10.1109/access.2020.2996093.

[3] Gai, K., Wu, Y., Zhu, L., Xu, L. and Zhang, Y. (2019). Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks. *IEEE Internet of Things Journal*, pp.1–1. doi:https://doi.org/10.1109/jiot.2019.2904303.

authorisation techniques to confirm user legitimacy, and establishes optimal security-aware strategies through smart contracts operating on the blockchain (Gai et al., 2019)[3].

2.4.3 Three-Layers Secure Access Control for Cloud-Based Smart Grids (Xie et al., 2015)[4]

This research explores the emerging trend of combining smart grids with cloud computing, and proposes a secure solution using a modified hierarchical attribute-based encryption (M-HABE) and an improved three-layer structure hierarchical access control method to ensure effective protection of data confidentiality and management permissions in a cloud-based hierarchical multi-user data sharing environment (Xie et al., 2015)[4].

2.4.4 Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid (Guan et al., 2017)[5]

This research introduces a ciphertext-secured data collection technique for smart grid. The process involves capturing data, segmenting it, and encrypting it in conjunction with corresponding access sub-trees. This strategy enables simultaneous data encryption and transmission. Furthermore, the research also highlights the use of a threshold secret sharing method during the encryption process to safeguard the confidentiality and security of user data. (Guan et al., 2017)[5]

2.4.5 Reflection on the "Identity" Issue of Endpoints and User in the Smart Grid

These research papers offer profound insights into the identity issue in smart grid. In terms of identity authentication, both the DRMAS certification scheme and the PBEM-SGN model propose advanced authentication mechanisms that can not only fend off known attacks but also complete the authentication process in a short time (Chaudhry et al., 2020)[2], (Gai et al., 2019)[3]. In terms of access control, the M-HABE and an improved three-layer structure hierarchical access control method ensure the data security (Xie et al., 2015)[4]. In terms of user and data privacy, the PBEM-SGN model utilises blockchain and edge computing technologies, and employs unique signature and authorisation techniques to safeguard user privacy (Gai et al., 2019)[3]. Additionally, the ciphertext-secured data collection technique also provides protection for the privacy of user data (Guan et al., 2017)[5]. These

[4] Xie, Y., Wen, H., Wu, J., Jiang, Y., Meng, J., Guo, X., Xu, A. and Guan, Z. (2015). Three-Layers Secure Access Control for Cloud-Based Smart Grids. [online] IEEE Xplore. doi:https://doi.org/10.1109/VTCFall.2015.7391174.

[5] Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J. and Du, X. (2017). Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid. IEEE Internet of Things Journal, 4(6), pp.1934–1944. doi:https://doi.org/10.1109/jiot.2017.2690522.

researches provide fresh insights and solutions to security issues in smart grid, facilitating the rapid development of smart grid.

3. The Layered Model

In this section, we will delve into a discussion around the layered model of the cloud-based information infrastructure proposed by Luo et al. (2016)[6]. Not only do we provide a comprehensive comparison between this proposed layered model and the OSI model, but we also contrast it with the centralised model, thereby providing detailed information for readers.

3.1 Comparisons between OSI Model and the Layered Model of the Cloud-based Information Infrastructure (Luo et al., 2016)[6], (Alani, 2014)[7]

Both the OSI model and the layered model of the cloud-based information infrastructure clearly define the functions of each layer and clearly demarcate boundaries, making the design and implementation of the model simpler and possessing a good hierarchical mechanism. However, due to the considerations of model design and different application domains, there may be significant differences in specific operation methods and details. In the following, we provide a comparison of the two models in several aspects, as shown in Table[1].

Table[1]. Comparisons between OSI Model and the Layered Model of the Cloud-based Information Infrastructure (Luo et al., 2016)[6], (Alani, 2014)[7]

	Open Systems Interconnection (OSI) model (Alani, 2014)[7]	Layered Model of the Cloud-based Information Infrastructure (Luo et al., 2016)[6]
Layers of Model	7 layers, including Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer	8 layers, including Power Fabric Layer, Sensor and Actuator Network Layer, Cyber Fabric Layer, Secure Communication Layer, Dynamical Scheduling Layer, Firmware Layer,

[6] Luo, F., Zhao, J., Dong, Z.Y., Chen, Y., Xu, Y., Zhang, X. and Wong, K.P., 2016. Cloud-based information infrastructure for next-generation power grid: Conception, architecture, and applications. *IEEE Transactions on Smart Grid*, *7*(4), pp.1896-1912.

[7] Alani, M.M., 2014. OSI model. *Guide to OSI and TCP/IP Models*, pp.5-17.

		Abstracted Service Layer, Power Application Layer
Purpose and Scope	Centred on understanding and describing how different network protocols interact during network communication.	Focused on managing resources, providing services, and ensuring security in cloud computing for power grid systems.
Complexity	Each layer's task is clearly defined and very explicit, making it easy to understand and implement.	Many details are considered, making it more complex and challenging to understand and implement compared to the OSI model.
Security	Security mainly involves data encryption and verification in the Presentation Layer and Application Layer.	A dedicated Secure Communication Layer is employed for data encryption and verification, further strengthening cybersecurity.
Resource Management	The focus is primarily on data transmission communication, without managing resources.	Resource allocation, load balancing, and data storage are implemented in the Dynamical Scheduling Layer.
Virtualisation Technology	Does not involve the use of virtualisation technology, focusing on the transmission process of network communication.	Virtualisation technologies are explicitly used in the Firmware Layer and Abstracted Service Layer, providing differentiated services to the power grid.
Grid Applications	Provides a general model without specific use in particular scenarios.	The model is clearly aimed at power grid systems, with support for power grid applications provided in the Power Application Layer.

3.2 Comparisons between Layered Models of Centralised vs. Distributed Cloud-Based Information Infrastructure

The layered models of centralised and distributed cloud-based information infrastructures may share the same layer structure. However, due to differing considerations in deployment environments and strategies, their specific operation methods and implementation details may significantly differ. In the following, we provide the differences between the layered models of centralised and distributed cloud-based information infrastructure, as shown in Table[2].

Table[2]. Comparisons between Layered Models of Centralised vs. Distributed Cloud-Based Information Infrastructure

	The Layered Models of Centralised Cloud-based Information Infrastructure	The Layered Models of Distributed Cloud-based Information Infrastructure
Resource Management	Most resources (devices and systems) are located in the same or a few locations, making them easier to monitor and manage, thus lowering the difficulty of resource management.	Resources are dispersed across data centres around the world, requiring more complex management strategies, thus making resource management more challenging.
Network Latency	As most servers or users are concentrated in neighbouring areas, the likelihood of network latency is relatively low.	Servers or users may be spread across different geographical locations, potentially leading to higher network latency.
Security and Privacy	Most data are stored in one location, and if it is attacked, it may lead to a large amount of data leakage, indicating lower security and privacy levels.	Data is dispersed across different regions, which can distribute the risk of data leakage, resulting in higher security and privacy.

Fault Tolerance	Most services rely on a few or a single data centre. If a problem arises, it could lead to a disruption of the entire system, indicating inferior fault tolerance.	Services rely on resources spread across multiple locations. If a data centre encounters a problem, it can quickly switch to another data centre, indicating superior fault tolerance.
Disaster and Failure Recovery	Data centre require robust backup and recovery strategies to handle single-point failures, resulting in lower disaster and failure recovery capabilities.	Services depend on resources spread across multiple locations. A single point of failure is less likely to affect the entire system, leading to higher disaster and failure recovery capabilities.

4. Threats

As the connectivity between endpoint devices and control systems in smart grid continues to strengthen, the need for cybersecurity correspondingly increases. Consequently, smart grid increasingly needs to address a variety of potential cybersecurity vulnerabilities. In the following, we outline three key cybersecurity vulnerabilities in smart grid:

4.1 Endpoint Vulnerabilities

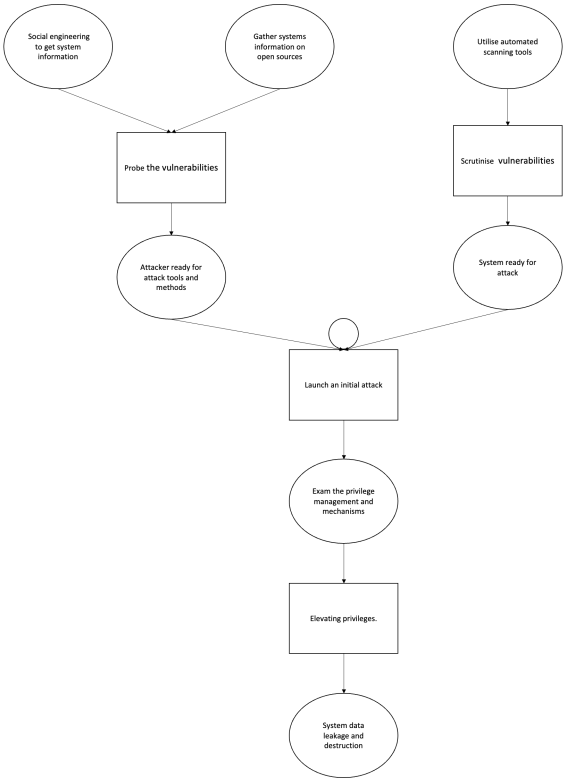
Smart grid contain many endpoint devices, such as smart meters and distributed energy devices. In this part, we discuss network connectivity at the endpoint and the physical security of endpoints. In terms of network connectivity, most of these endpoint devices are connected to networks, providing many opportunities for attackers to intrude. In terms of physical security, these endpoint devices may be located in remote or unguarded areas, vulnerable to malicious individuals exploiting interfaces to implant malware or viruses, thereby stealing sensitive data and gaining control.

4.2 Communication Vulnerabilities

In smart grid, good network communication allows for the secure transmission of vast amounts of data between devices and users. In this part, we discuss data encryption and authentication mechanisms. In terms of data encryption, if data is not properly encrypted with secure algorithms and protocols, it is likely to be easily intercepted and decrypted by attackers for a man-in-the-middle attack. In terms of authentication mechanisms, endpoints and users need a robust authentication and access control system to prevent attackers from sabotaging the mechanism and masquerading as legitimate devices or personnel.

4.3 System Vulnerabilities and Attack Graph

The control systems of intelligent power grid need to process massive amounts of data and make real-time decisions. In this part, we discuss the security of system software and hardware components, as well as system security configurations. When it comes to the security of software and hardware components, if these intelligent power grid control systems are not continuously updated to the latest versions, attackers can gather system information to discover vulnerabilities and conduct attacks. Regarding system security configurations, improper permission settings could lead to an imbalance of device and user permissions and expose services and ports, allowing attackers to exploit vulnerabilities through vulnerability scanning. Furthermore, we follow the attack graph proposed by Lallie et al. (2018)[8], and provide attack graph of system vulnerabilities, as shown in Figure[1].


Social engineering to get system information
Gather systems information on open sources
Utilise automated scanning tools
Probe the vulnerabilities
Scrutinise vulnerabilities
Attacker ready for attack tools and methods
System ready for attack
Launch an initial attack
Exam the privilege management and mechanisms
Elevating privileges.
System data leakage and destruction

Figure[1]. Attack Graph of System vulnerabilities (Lallie et al., 2018)[8]

[8] Lallie, H.S., Debattista, K. and Bal, J., 2018. Evaluating practitioner cyber-security attack graph configuration preferences. Computers & Security, 79, pp.117-131.

5. Conclusion

Given the numerous advantages of smart grid, such as bidirectional communication and real-time monitoring, an increasing number of countries are transitioning from traditional grid to smart grid. This transition is preparing their power systems to better serve the society of the future.

After a thorough understanding of the layered model of cloud-based information infrastructure, and the threats and vulnerabilities of cybersecurity, we have realized that smart grid and cloud-based information infrastructure are closely related. With the advantages of the cloud, the smart grid can perform large-scale data calculations and better integrate endpoints in the grid. However, despite the cost benefits, high scalability, and convenience offered by cloud computing, it is not suitable for all power applications. This is largely due to certain inherent disadvantages of the cloud. In the following, we present a few power applications that should not be migrated to the cloud:

Real-time monitoring systems: In a cloud environment, network latency is inevitable. For instance, SCADA systems in power grid need to act within a very short time to ensure grid stability and security. Furthermore, the cloud environment diminishes data security. The data of these systems is extremely sensitive; any unauthorized access or tampering could cause massive losses and impacts to the grid.

Power management systems: Power management systems are responsible for monitoring and controlling devices in the power grid, including servers, energy storage devices, modems, etc. To allow these devices to run accurately and efficiently, power management systems must be able to react promptly and hence are not suitable for migration to the cloud. Moreover, if control instructions from power management systems are illegally intercepted and tampered with, this could lead to large-scale power outages and data loss.

In summary, smart grid and cloud-based information infrastructure are closely related. With the convenience of cloud computing, endpoints in the power grid can access and interconnect a large amount of data, thereby enhancing the overall performance and reliability of the power grid. However, not all grid applications should be migrated to the cloud due to considerations of system security and data confidentiality. Before considering migration, a thorough assessment of the application requirements and cloud characteristics is required to ensure that systems within the grid can maintain data security and system stability.