People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research

University of Abdelhamid Mehri – Constantine 2

Faculty of New Technologies of Information and Communication (NTIC)

Department of Fundamental Computing and its Applications (IFA)

MASTER'S THESIS

to obtain the diploma of Master degree in Computer Science

Option: Sciences and Technologies of Information and Communication (STIC)

Cybersecurity of smart grid infratsructure communication

Realized by:

ochetati ilyes chiheb eddine

kechicheb ahmed

Under supervision of:

Salim benayoune

June 2024

بسم الله الرحمن الرحيم

Chapter

1

State of the Art

Introduction

Electricity grids, commonly referred to as "grids," play a vital role in modern energy infrastructure. They facilitate power generation, transmission, distribution, and control. Over time, grids have evolved from localized systems to interconnected networks, adapting to meet increasing demands and technological advancements. These grids contribute significantly to economic and societal progress.

Amidst dynamic changes in the energy landscape, the emergence of the "smart grid" presents transformative possibilities. Leveraging data, automation, and connectivity, smart grids enhance energy management and promote sustainability. In this chapter, we delve into the evolution of grid systems and explore the challenges and opportunities associated with smart grid technology, shaping the future of energy.

1.1 Definition smart grid

The Smart Grid is a comprehensive electrical network that employs cutting-edge communication technologies, computational intelligence, and cybersecurity protocols throughout the entire process of generating, transmitting, distributing, and consuming electricity. Its objective is to establish a system that is environmentally friendly, secure, dependable, adaptable, energy-efficient, and environmentally sustainable. While the ultimate vision of the Smart Grid is ambitious, its practical implementation demands careful evaluation of costs, rigorous testing, and validation. Introducing new functionalities can occur autonomously, with each necessitating justification and a reasonable return on investment. The compatibility of open systems facilitates smooth integration into the Smart Grid once the technologies have been validated [1]. The National Institute of Standards and Technology (NIST), operating within the U.S. Department of Commerce, has classified the smart grid into seven distinct domains, as illustrated in Figure 1.1. A concise overview of these domains and their stakeholders is provided in Table 1.1.[2]

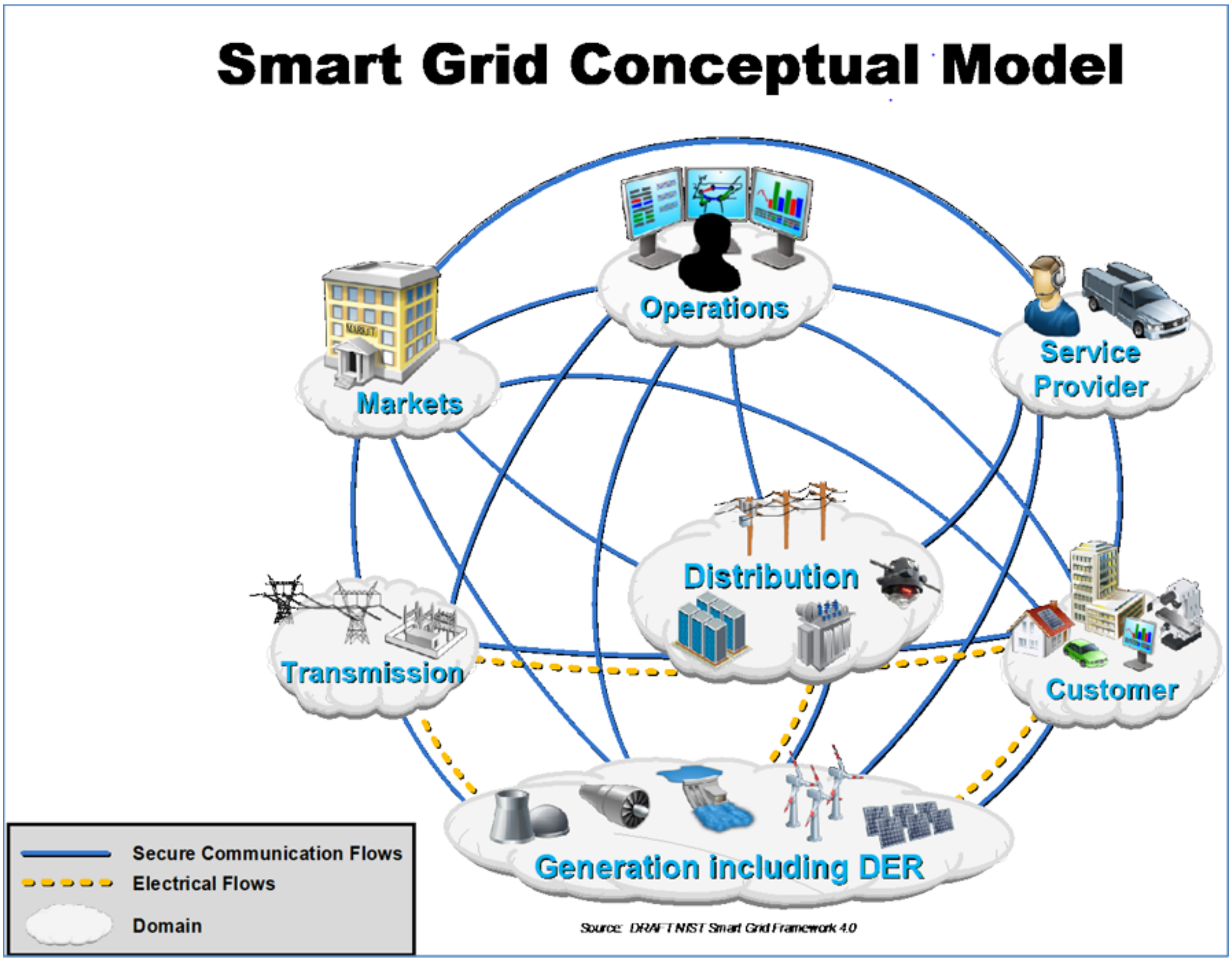

Figure 1.1: The NIST Conceptual Model for SG [2]

Domain	Roles/Services in the Domain
1 Customer	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own sub-domain: residential, commercial, and industrial.
2 Markets	The facilitators and participants in electricity markets and other economic mechanisms used to drive action and optimize system outcomes.
3 Service Provider	The organizations providing services to electrical customers and to utilities.
4 Operations	The managers of the movement of electricity.
5 Generation Including DER	The producers of electricity. May also store energy for later distribution. This domain includes traditional generation sources and distributed energy resources (DER).
6 Transmission	The carriers of high voltage electricity over long distances. May also store and generate electricity.
7 Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

Table 1.1: Domains and their associated roles/services [2]

1.2 Smart grid attributes

Many smart grid advocates cite some or all of its following attributes as representative of its promise:

- **Efficiency:** Capable of meeting growing consumer demand without the need for additional infrastructure.
- **Flexibility:** Able to accept energy from various sources, including solar and wind, with the same ease as traditional fuels like coal and natural gas. It can integrate new technologies, such as energy storage, as they become commercially viable.
- **Empowering:** Facilitating real-time communication between consumers and utility providers, allowing consumers to adjust their energy usage based on factors like price and environmental concerns.
- **Opportunistic:** Creating new markets and opportunities by leveraging plug-and-play innovations whenever suitable.
- **Focus on Quality:** Able to deliver reliable power without disruptions, ensuring the smooth operation of digital technologies crucial to our economy.
- **Resilience:** Increasingly resistant to cyber attacks and natural disasters through decentralization and the implementation of smart grid security measures.
- **Environmental Sustainability:** Contributing to the mitigation of climate change

and offering a viable path towards reducing the environmental impact of electricity generation. [3]

1.3 Differences between Traditional grid and Smart grid

Table 1.2 offers a thorough comparison of the conventional power grid with the smart grid. In contrast to the traditional grid where customers play a passive role, the smart grid actively engages them through bi-directional communication technologies. For instance, rooftop photovoltaic solar panels produce electricity during the day, enabling customers to sell surplus energy back to the grid. At night, these panels continue to power home appliances as usual. Moreover, the smart grid incorporates innovative technologies like distributed generation, electric vehicle charging and discharging, and Flexible Alternating Current Transmission Systems (FACTS) to improve energy distribution and management.[4]

Table 1.2: Comparison between conventional grid and smart grid [5]

Aspects	Conventional Grid	Smart Grid
Interaction between Grid and Customers	Customers passively accept service from grid	Customers participation on the grid action
Renewable Energy Integration	Having trouble with renewable penetration	Integration with renewable resources enhancement
Options for Customers	No choice for customer, monopoly market	With digital market trading, PHEV, introduce bids and competition, more choice for customer
Options on Power Quality (PQ)	No choice on power quality, no price plan options for consumers	Power quality levels for different consumers
System Operation	Ageing power assets, no efficient operation	Assets operating optimization, less power loss
Protection	Only rely on protection devices, fault detect manually	Have capability of self-healing, less damage affected by fault
Reliability and Security	Susceptible to physical and cyber attack	More reliable for national security and human safety

1.4 Major systems

1.4.1 Smart infrastructure system

The smart infrastructure system consists of three main components: the smart energy subsystem, the smart information subsystem, and the smart communication subsystem. Within the smart energy subsystem, activities such as electricity generation, transmission, distribution, and consumption are integrated. The smart information subsystem includes functions like smart metering and advanced monitoring and management of the smart grid network. The smart communication subsystem facilitates wired and wireless communication between networks, devices, and applications to establish connectivity throughout the network [6].

1.4.2 Smart management system

The smart grid's intelligent management system offers advanced services in monitoring and control. As innovative management, monitoring, and control applications evolve, smart grid technology becomes more sophisticated, contributing actively to the advancement of a sustainable power system. Within the smart management system are functions such as enhancing energy efficiency, balancing supply and demand, controlling emissions, reducing operational costs, and maximizing utility. This system utilizes modern machine learning and optimization tools to create a resilient and efficient smart management framework [6].

1.4.3 smart protection systems

The smart protection system within the smart grid offers services related to reliability, safeguarding against failures, and ensuring security and privacy. By incorporating advanced protection devices and monitoring tools, the system enhances the reliability, security, and privacy of the network. Alongside smart infrastructure planning, efficient management, and intelligent protection systems play a role in managing operations effectively, protecting against failures, and addressing cybersecurity and privacy concerns within the network. Figure 1.2 illustrates a typical technological framework of the smart grid [6].

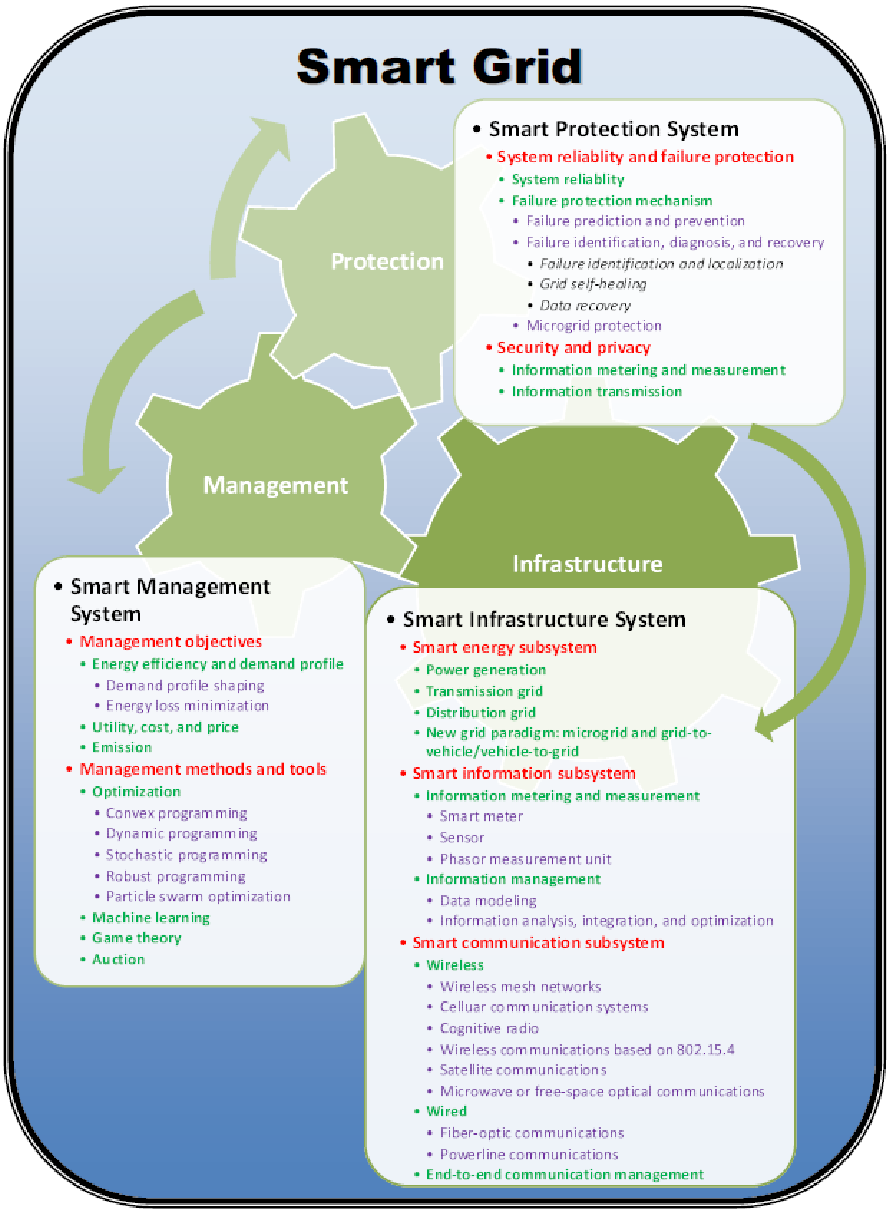

Figure 1.2: Classification of the Smart Infrastructure System, the Smart Management System, and the Smart Protection System [7]

1.5 Smart Grid Technologies

A smart grid employs a diverse array of technologies and communication networks to enhance the management of power generation, transmission, and distribution. It also provides customers with the ability to have real-time control over their energy consumption [8].

1.5.1 Major Smart Grid Technologies

1.5.1.1 Advanced Demand Forecasting

Utilizing data analytics and machine learning (ML), advanced demand forecasting techniques produce forecasting reports through autoregressive integrated moving average (ARIMA) and various statistical methods.

A crucial aspect of smart grid management, ARIMA forecasting predicts both annual electricity consumption and hourly electricity prices.

Furthermore, ARIMA forecasting serves as an extra layer of verification, aiding in the identification of cyber intrusion attempts on smart meters used to measure electricity usage for residential and commercial consumers [8].

1.5.1.2 Advanced Metering Infrastructure (AMI)

Advanced Metering Infrastructure (AMI) is a unified system comprising communication networks, data management systems, and intelligent meters designed to enhance customer service, energy efficiency, and cost management.

AMI facilitates two-way communication between customers and utilities, offering a wide array of advantages to the smart grid. These include forecasting consumption, improving revenue collection and theft detection, detecting faults and outages, measuring losses, and implementing time-based pricing [8].

1.5.1.3 Big Data

Smart grid data possesses three fundamental characteristics: high velocity, extensive volume, and diverse variety. Managing this large volume of data in a timely manner with limited resources poses a significant challenge for smart grids. This is where big data analytics becomes pivotal, offering the potential to boost asset utilization, efficiency, system reliability, and customer satisfaction.

Without big data analytics in the smart grid, the assessment of petabytes of data generated by smart grid devices would be impractical. Big data captures and analyzes unstructured data from various endpoints within a smart grid.

Moreover, big data facilitates efficient cost reduction, optimal resource distribution, and improved customer service [8].

1.5.1.4 Distributed Energy Resources (DERs)

Distributed Energy Resources (DERs) supply energy and improve local reliability, enhancing grid stability and optimizing on-site fuel utilization.

DERs encompass various technologies such as electric vehicles, solar panels, small natural gas generators, and controllable loads like electric water heaters and HVAC systems.

Efficient integration of DERs enhances grid service quality and reliability. For instance, photovoltaic systems (PVs) utilize the photovoltaic effect to convert sunlight into electricity, which is then transformed into alternating current by an inverter. The primary advantage of PV systems is reduced utility bills due to decreased reliance on grid-provided electricity [8].

1.5.1.5 Non-intrusive Load Monitoring (NILM)

Non-intrusive load monitoring (NILM), also known as non-intrusive appliance load monitoring (NIALM), discerns the specific energy consumption of households and industrial sites.

By disaggregating the total energy usage (from active appliances) into individual components and offering diagnostic insights, NILM aids in identifying energy-intensive or faulty appliances.

Moreover, consumers can optimize the timing of usage for energy-intensive appliances to minimize costs, and monitor and control energy expenses based on their power consumption [8].

1.5.1.6 Vehicle-to-Grid (V2G)

Also known as vehicle-grid integration (VGI), vehicle-to-grid (V2G) technology transfers unused power from a vehicle into the smart grid. An electric vehicle (EV) battery is a cost-efficient form of energy storage.

V2G helps balance electricity consumption spikes and reduce overload on the power grid during peak hours.

For example, V2G can feed energy (unused battery capacity) back to the power grid from an electric car's battery to improve grid stability and maximize the benefits of renewable energy [8].

1.5.2 Established and Emerging Smart Grid Communication Networks

1.5.2.1 HAN

A smart meter supplies power to household appliances via the Home Area Network (HAN), which utilizes different technologies such as Bluetooth, Wireless Ethernet, Wired Ethernet, and Zigbee. The HAN links home appliances with the smart meter, which detects power usage and transmits this information to the server for billing purposes [8].

1.5.2.2 NAN

A Neighborhood Area Network (NAN) is an external access network that links distribution automation devices and smart meters to WAN gateways such as RF (radio frequency) collectors and field devices (like Intelligent Electronic Devices (IEDs)). NAN allows for customer data collection and facilitates communication within the WAN-premise area [8].

1.5.2.3 WAN

A wide area network (WAN) uses fiber optics, 3G/LTE (Long Term Evolution)/GSM (Global System for Mobile Communication), or WiMAX (Worldwide Interoperability for Microwave Access) for communication between a smart meter, suppliers, and the utility server. A smart meter sends notifications it receives (via HAN) from the devices to the suppliers using WAN [8].

1.5.2.4 LoRaWAN

LoRa (Long Range) is a popular IoT (Internet of Things) technology known for its long-range capability and low-power wireless platform, making it well-suited for various applications including energy management, infrastructure efficiency, and disaster prevention.

Implementing smart electricity metering solutions and smart grid networks using the LoRaWAN® (Long Range Wide Area Network) protocol allows for improved understanding of power demand, efficient detection of power outages, enhanced connectivity, and identification of underperforming assets.

Additionally, LoRaWAN is globally compatible and ensures seamless transmission without interference for remote reading of heat meter consumption data [8].

1.6 Components of the Smart Grid

There are many components, but will talk about the most important ones.

1.6.1 Smart Meters

The interplay between smart meters and smart grids is depicted in Figure 1.3. From the perspective of the smart grid, the applications primarily revolve around leveraging smart meters to facilitate the coordination of various electrical devices, thereby achieving a dependable power system. Simultaneously, these applications strive to enhance the performance and efficiency of smart metering. These objectives align with the defining characteristics of smart grids, which drive the advancement of smart meter technologies.[9]

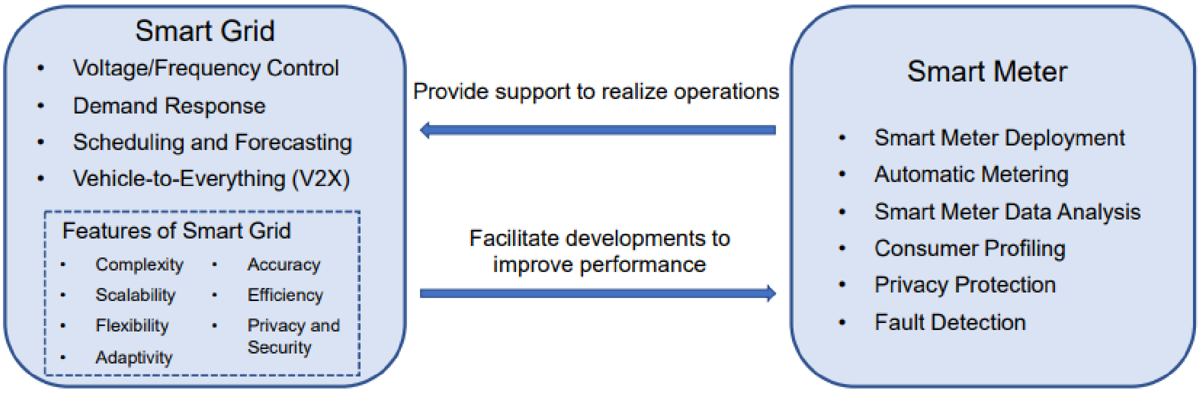

Figure 1.3: Applications from smart grid and smart meter perspectives. [9]

1.6.2 Advanced Distribution Management Systems

An ADMS is a software platform designed to support the comprehensive suite of tasks related to managing and optimizing the distribution of electricity. It encompasses functions that automate outage recovery and enhance the effectiveness of the distribution grid. These functions being developed for electric utilities include fault location, isolation, and restoration; optimization of voltage and reactive power; energy conservation through voltage reduction; management of peak demand; as well as support for microgrids and electric vehicles [10].

1.6.3 Super conducting cables

These components are utilized for transmitting electricity over extended distances and employing automated monitoring and analysis tools. These tools have the capability to identify faults independently or predict potential cable failures by analyzing real-time data, weather conditions, and the history of outages [11].

1.6.4 Circuit breakers

The circuit breaker, a safety-conscious middle-aged individual, safeguards the power system. It evaluates smart grid scenarios against safety standards, offering recommendations. Despite occasional differences, both the smart grid and circuit breakers recognize their mutual importance. Their relationship ensures the power system's safe and stable operation.

Smart Grid occasionally proposes innovative features or adjustments to the power system. However, the breaker gently dissuades excessive risk-taking, emphasizing safety.

Through discussions and disputes, they strike a balance, ensuring reliable electricity for our lives [12].

1.6.5 Collector nodes

Collector nodes are pivotal in the Smart Grid, serving as points of data collection and distribution between energy suppliers and customers. They enable a two-way communication network within the grid, relaying information from customer premises to the utility control center and transmission/distribution substations. Collector nodes facilitate efficient monitoring and management of energy usage [13].

1.7 Challenges and Considerations

1.7.1 Stakeholder Engagement

At the early stages of smart grid implementations, stakeholders' negative perceptions can derail even the most beneficial project, especially when the proponents fail to pay close attention to the educational aspects. Advocates need to be able explain and clearly identify the benefits of each component of the smart grid to the customers that are the potential key to service success [3].

1.7.2 Fear of obsolesce

As many technology users (computers, smart phones, etc.) are painfully aware, the adoption of new tools can open the door to new and additional costs that may only be borne by the eventual consumer. This fear can be addressed through the development of interoperability standards and backward compatibility of technologies [3].

1.7.3 Cybersecurity

Without a shred of doubt, cybersecurity stands out as one of the foremost and intricate challenges confronting IoT devices. Sensors, devices, and networks connected to the internet are persistent targets for various online threats like probing, espionage, ransomware, theft, and potential destruction. Considering that an IoT-driven smart grid can encompass potentially millions of interconnected nodes spread across extensive geographic regions, it emerges as the most susceptible to substantial cyber assaults. Consequently, a cyber-attack on such a system would have devastating consequences, leading to significant financial losses and potentially bringing entire countries to a standstill. The diagram in Figure 1.4 illustrates the number of articles reviewed per year of publication and smart grids impacted by cyber-attacks. Hence, security stands as a major hurdle in both the deployment and operation of IoT-based smart grid networks.[14].

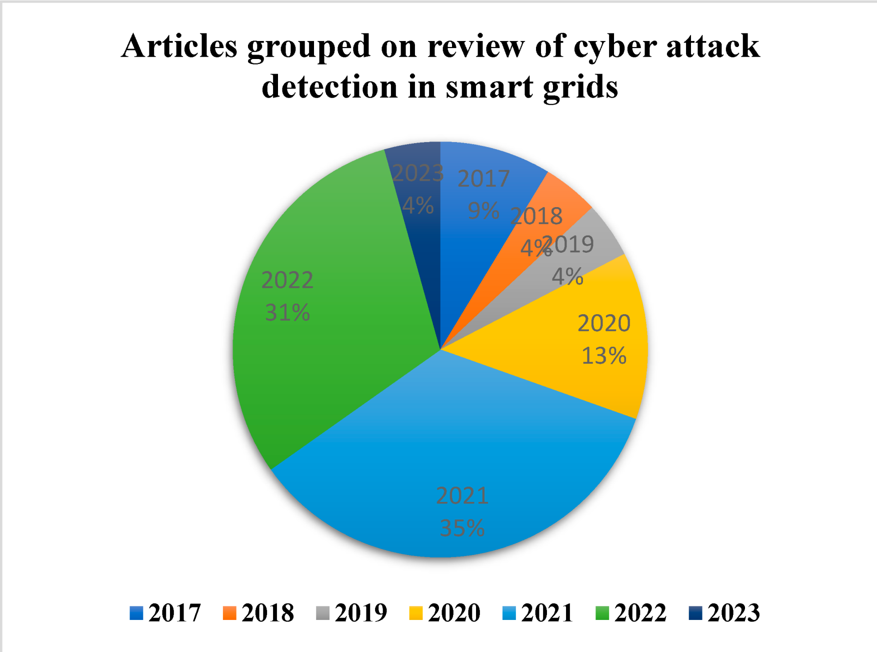

Figure 1.4: Estimate: cyber attacks will increase exponentially [15]

1.7.4 Data privacy

Privacy is a critical concern within smart grid networks, prompting significant questions about the creation of policies regarding user data privacy. These questions revolve around several key points: Who owns the customer data? How is access to and usage of customer data regulated? What measures exist to protect the privacy and security of customer data from potential risks like surveillance or illicit activities? Is it permissible to sell or transfer customer data, and under what circumstances and for whose benefit? In areas with retail choice, are measures necessary to ensure that competing electricity providers have equal access to customer data compared to the incumbent utility?

In competitive environments among electricity providers, access to users' electricity usage patterns and behavioral information holds significant importance. Providers or their representatives may use this data to develop business strategies and create tailored packages or offers. In an open market scenario, some data may be disclosed after offers are made public, providing a level playing field for information access. However, if privacy is compromised beforehand, with specific user data available to only certain parties, these electricity providers could potentially gain unfair advantages. Therefore, effective privacy policies are essential to prevent the exploitation of unfair means in shaping business strategies.

The integration of Information and Communication Technologies (ICTs) into smart grid operations introduces various privacy concerns. Depending on how a consumer uses and recharges electricity [16].

1.7.5 Cost of Implementation:

Estimating Smart Grid costs poses challenges due to several factors. Integrating digital technology into Smart Grids introduces complexities, as the failure rates and life expectancy of embedded assets differ from traditional grid technologies. For instance, a substation transformer designed for 40 years may be coupled with information technology lasting 10, 15, or 20 years, necessitating careful cost considerations for upgrades. Additionally, the rapid obsolescence of digital tech complicates estimates, as advancing communications and computational capabilities may render Smart Grid components obsolete before their intended lifespan ends.

Moreover, the evolution of Smart Grid technologies is expected to outpace conventional tech in terms of cost reduction and advancements. However, uncertainties persist, particularly with new and unproven Smart Grid technologies. If their performance is subpar or degrades unexpectedly, it could jeopardize the entire technology's viability and business plan. As Smart Grid component costs decrease rapidly due to maturation and increased production, estimating replacement costs becomes challenging[17].

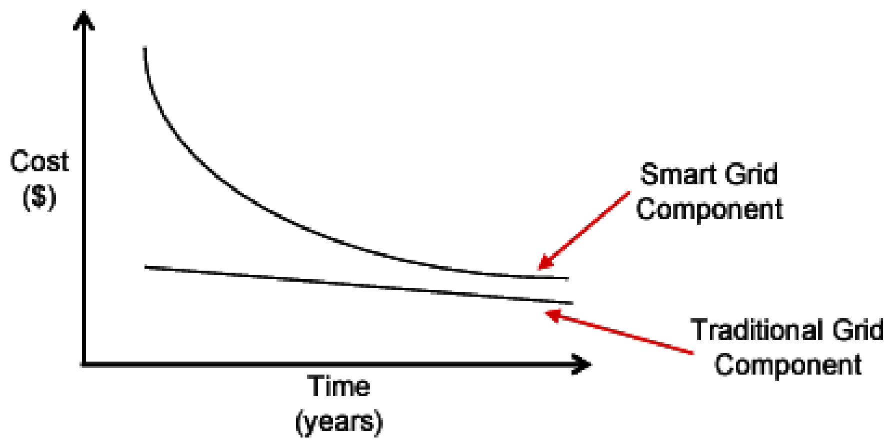

Figure 1.5: Grid Component Costs [17]

1.7.6 Regulatory Frameworks

Electric distribution systems across Europe are encountering significant hurdles stemming from climate change objectives, evolving market frameworks, and technological advancements. These factors will have a profound impact on the responsibilities of distribution system operators. The challenges' nature and magnitude are primarily influenced by Europe's vision and strategies regarding climate and energy. This research aims to identify which policies might pose obstacles to innovation in distribution grids and the adoption of advanced smart grid solutions developed within the UNITED-GRID project. Following an in-depth examination of emerging policy priorities within the energy and climate framework, as well as electricity market design, and subsequent consultations with three partner distribution system operators, five key barriers have been pinpointed. The findings indicate that ambitious decarbonisation targets and shifting expectations regarding the role of distribution system operators in the energy landscape necessitate more adaptable and efficient network management. However, rigid income frameworks, insufficient incentives for innovation, and regulatory uncertainties impede the modernisation of distribution systems. It can be inferred that these concerns heighten the risks for distribution system operators and must be taken into account by research initiatives and developers of smart grid solutions to successfully implement and achieve market adoption of the developed solutions [18].

Conclusion

The smart grid revolution is not a destination, but a continuous journey towards a more efficient, reliable, and sustainable energy future. While challenges exist, the potential benefits of the smart grid are undeniable. By embracing innovation, fostering collaboration, and empowering consumers, we can unlock the full potential of this transformative technology.

A smarter grid paves the way for a future where clean energy sources like solar and wind power are seamlessly integrated, homes and businesses actively participate in energy management, and power outages become a rarity. It's a future where we have a more secure and sustainable energy infrastructure for generations to come.

Let's continue exploring the exciting world of smart grids and work together to build a brighter energy future for all.

Chapter 2

Contributions

Introduction

With the birth of the smart grid as the next step of evolution for grid infrastructure, with the improvements that the smart grid came with, like improved reliability, automation, and faster detection and response to failures, it also came with its own set of risks and disadvantages. mainly due to the fact that it is composed of multiple components and systems that are connected to the internet, like wireless networks and sensors, smart meters, and IoT devices, making it an easy target for hackers. independent groups or state actors whose goal is to cause as much damage as possible or to collect valuable data. On top of those components, there are legacy systems that the smart grid relies on that are known for their many and major security vulnerabilities, which are all easy targets, for example, Supervisory Control and Data Acquisition (SCADA). As an example of those risks and weaknesses, we can look at the situation Ukraine found itself in after Russia targeted their smart grid systems in 2015, leaving 80,000 Ukrainian households without power for 3 to 6 hours. [19].

That's why it is important to protect the smart grid system from cyberattacks by employing IDS, IPS, and IDPS. as the second line of defense in case encryption and authorization were unsuccessful in stopping the cyberattack from targeting the smart grid system.

2.1 Intrusion detection systems (IDS)

An intrusion detection system is a piece of hardware or software that is responsible for detecting suspicious and malicious activity, and in a network or an information system, the anomaly can either be reported to a systems administrator or saved to a security information and even management system (SIEM), the SIEM combines the output from multiple sources, then uses some filtering techniques to decide if the reported activity is malicious. [20]

2.2 Intrusion detection systems architecture

Intrusion detection systems, like any complex system, are made of multiple interoperating components with a specific task assigned to each component. Although the functioning of an IDS changes vastly between different types of IDSs (diffrent in deployment or detection methods), they all share a common general architecture, which is composed of the following components as shown in Figure 2.1 [21]:

- Data gathering components (sensor): tasked with collecting information from the monitored environment.
- Detector (IDS engine): analyzes the data collected by the sensor to determine the presence of suspicious activity.
- Knowledge base(database): the database that stores information collected previously by sensors about known attacks that allows the engine to determine the suspesious activity.
- Configuration component: defines settings and the behavious of the system.
- Response component: this component is responsible for responding to the detected intrusion and either attempts to prevent the intrusion (IPS) or reports it to a human administrator (IDS).

2.3 Intrusion detection systems classification

Intrusion detection systems are classifeied according to 2 criterias of classification which as shown in Figure 2.2 are:

- deployment method:
- detection method:

[22]

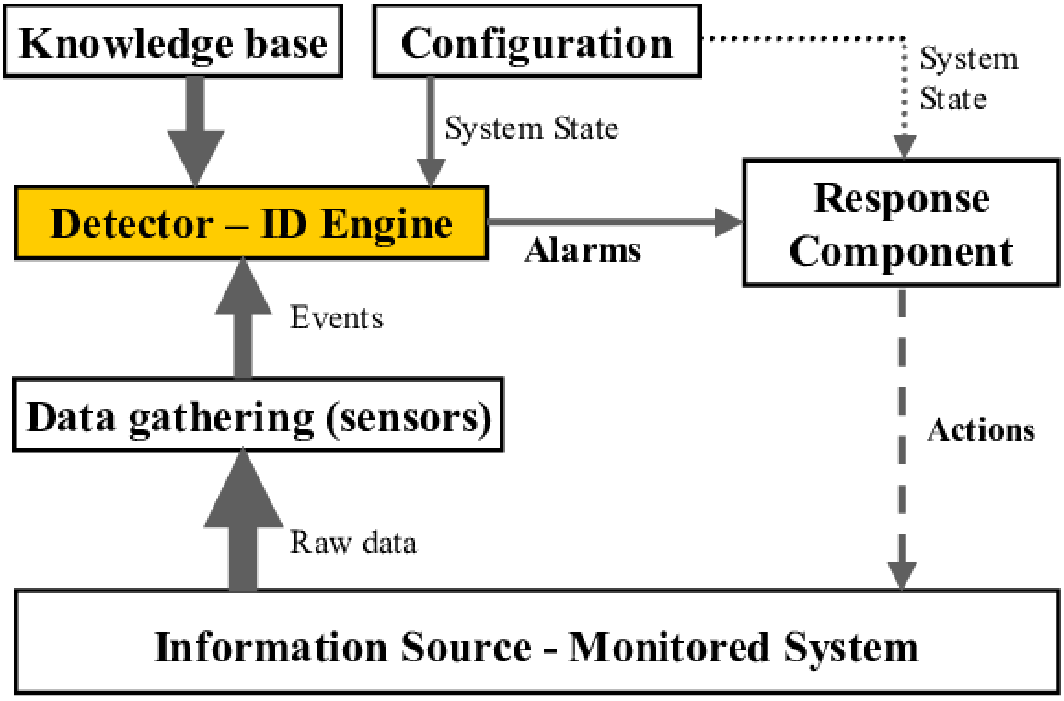

Figure 2.1: arch IDS

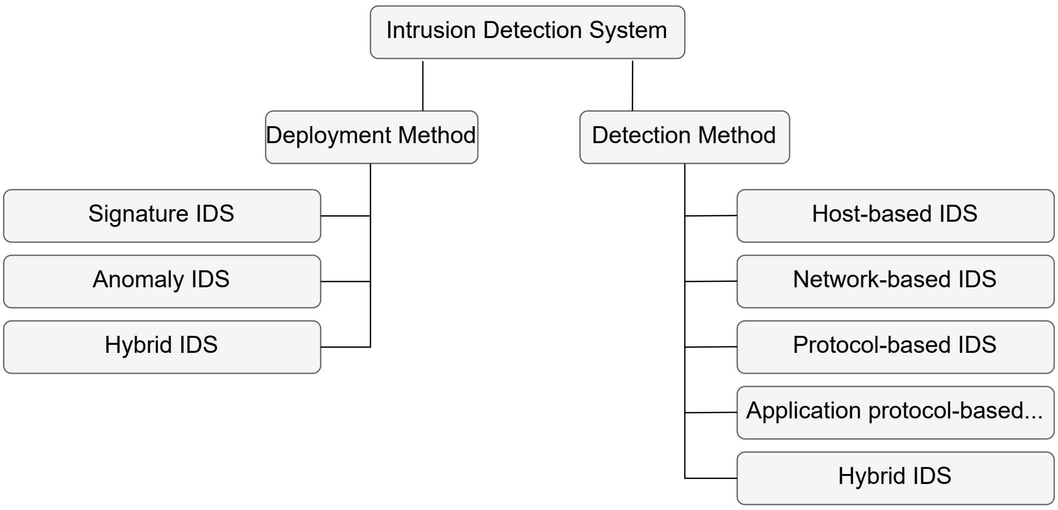

Figure 2.2: IDS classification taxonomy

2.3.1 Deployment methods

2 primary are HIDS and NDIS

some more specialized methods PIDS APIDS and hybrid https://www.ibm.com/topics/intrusion-detection-system

2.3.1.1 NIDS

Network intrusion detection systems are the most commonly used commercial IDS. They are usually placed at the start edge of the sub-network, right after the firewall (if one exists), so they can have access to all inbound traffic to all devices on the network [23]. NIDS protects the networks from cyber attacks and threats by scanning and monitoring TCP/IP packets for known attack signatures and reporting them to the administrator [24]

Some benefits of using a NIDS are that a few well-placed NIDS can be enough to cover an entire large network. In addition, their deployment requires minimal refactoring of the network, meaning easy installation [23]. But the downsides are that they cannot detect threats with inaccurately constructed attack signatures and cannot analyze encrypted traffic, and it is hard to work with networks operating at 10 Gbps [24].

With a NIDS, one would ideally scan all inbound and outbound traffic; however, doing so might create a bottleneck that would impair the overall speed of the network.

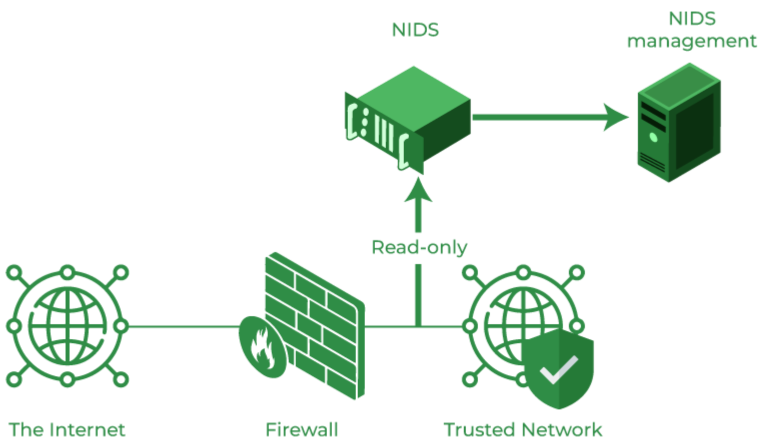

Figure 2.3: NIDS [25]

2.3.1.2 HIDS

Unlike NIDS, HIDS run on individual devices in a network, making it's threat detection scope more focused. They monitor all incoming and outgoing traffic and alert the administrator if suspicious or malicious activity is detected.

It is considered to be more reliable than NIDS because it has access to files in the operating system, and it can detect if a file has been tampered with by keeping snapshots of previous versions of those system files and comparing them to the current version to decide if it has been tampered with. [23]

This type of IDS uses 2 sources of information inside the device's operating system:

- system audit trails: operating system audit trails are created by the kernel making them very detailed because the kernel has access to everything in an OS. [23]
- system logs: less complex the system audit trails making them easier to understand. [23]

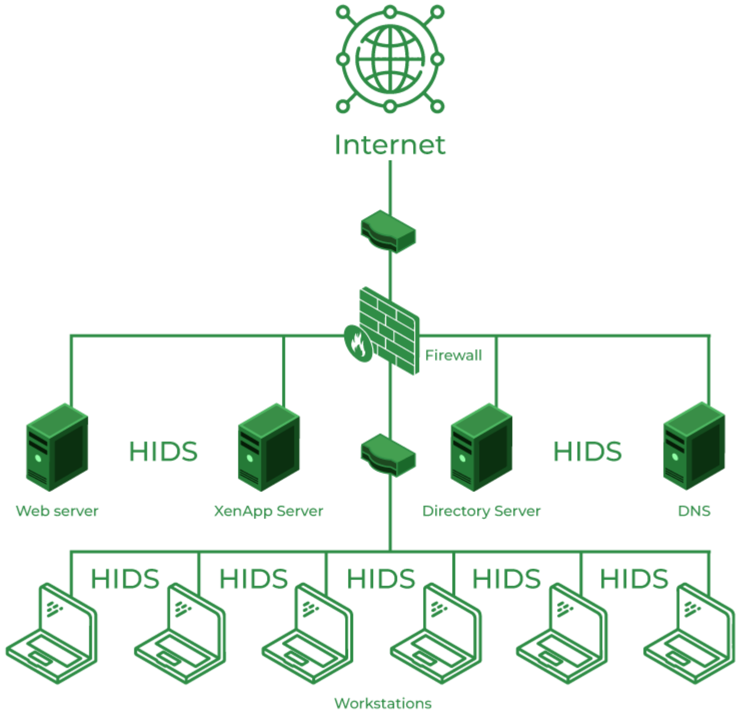

Figure 2.4: HIDS [25]

2.3.1.3 PIDS

2.3.1.4 APIDS

2.3.1.5 Hybrid IDS

2.3.2 Detection methods

there are 2 primary methodes of detection for IDS which are anomaly-based and signature-based which is also known as misuse intrusion detection or knowledge-based intrusion detection [22]

2.3.2.1 Signature-based detection

SIDs define patterns in known cyberattacks and store them in a database as signatures. The SID then analyzes system activity and search for a pattern of suspicious activity that matches previously documented attacks's signatures. This method provides high detection capabilities against known attacks. even though it cannot detect new attacks.On top of that, the database of previous attacks is very large, and having to compare internet packets to this database is resource- and time-consuming. [23]

2.3.2.2 Anomaly-based detection

2.3.2.3 Hybrid detection

is in development

2.4 maybe comparison between methodes of detection and deployment

2.5 maybe IDS vs IPS + IDPS

2.6 maybe IDS usage in smart grid

2.6.1 maybe IDS requirements

2.6.2 maybe IDS importance

2.7 conclusion

Chapter

3

Implementation

Bibliography

[1] Hamid Gharavi and Reza Ghafurian. *Smart grid: The electric energy system of the future*, volume 99. IEEE Piscataway, NJ, USA, 2011.

[2] Avi Gopstein, Cuong Nguyen, Cheyney O'Fallon, Nelson Hastings, David Wollman, et al. *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology . . . , 2021.

[3] Mohamed E El-Hawary. The smart grid—state-of-the-art and future trends. *Electric Power Components and Systems*, 42(3-4):239–250, 2014.

[4] Haotian Zhang. *Smart Grid Technologies and Implementations*. PhD thesis, City University London, 2014.

[5] Joe Miller. Understanding the smart grid: Features, benefits and costs. In *Illinois Smart Grid Initiative–Workshop*, 2008.

[6] GM Shafiullah, Aman Maung Than Oo, ABMS Ali, and Peter Wolfs. Smart grid for a sustainable future. 2013.

[7] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid—the new and improved power grid: A survey. *IEEE communications surveys & tutorials*, 14(4): 944–980, 2011.

[8] Blackridge Research. What is a smart grid? what are the major smart grid technologies? URL `https://www.blackridgeresearch.com/blog/what-is-a-smart-grid-what-are-the-major-smart-grid-technologies#smart-grid-technologies`. Accessed on 22 April 2024.

[9] Zhiyi Chen, Ali Moradi Amani, Xinghuo Yu, and Mahdi Jalili. Control and optimisation of power grids using smart meter data: A review. *Sensors*, 23(4):2118, 2023.

[10] Artur R Avazov and Liubov A Sobinova. Advanced distribution management system. In *EPJ Web of Conferences*, volume 110, page 01004. EDP Sciences, 2016.

[11] ElProCus. Overview of smart grid technology, operation & application in existing power system. URL https://www.elprocus.com/overview-smart-grid-technology-operation-application-existing-power-system/. Accessed on 20 April 2024.

[12] Lena Wang. Smart grids and circuit breakers: The tale of two happy enemies. URL https://www.linkedin.com/pulse/smart-grids-circuit-breakers-tale-two-happy-enemies-lena-wang-iuy1c?trk=article-ssr-frontend-pulse_more-articles_related-content-card. Accessed on 20 April 2024.

[13] Yu Cunjiang, Zhang Huaxun, and Zhao Lei. Architecture design for smart grid. *Energy Procedia*, 17:1524–1528, 2012.

[14] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. Cyber security challenges for iot-based smart grid networks. *International journal of critical infrastructure protection*, 25:36–49, 2019.

[15] Link to mdpi article. URL https://www.mdpi.com/1996-1073/16/4/1651. Accessed on April 20, 2024.

[16] Sherali Zeadally, Al-Sakib Khan Pathan, Cristina Alcaraz, and Mohamad Badra. Towards privacy protection in smart grid. *Wireless personal communications*, 73:23–50, 2013.

[17] U.S. Department of Energy. Estimating the costs and benefits of the smart grid: A preliminary estimate, 2011. URL https://smartgrid.gov/files/documents/Estimating_Costs_Benefits_Smart_Grid_Preliminary_Estimate_In_201103.pdf. Accessed on 20 Avril 2024.

[18] Joni Rossi, Ankur Srivastava, David Steen, and Le A Tuan. Study of the european regulatory framework for smart grid solutions in future distribution systems. In *CIRED 2020 Berlin Workshop (CIRED 2020)*, volume 2020, pages 800–802. IET, 2020.

[19] GROUPE DE TRAVAIL CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS. Fiches incidents cyber si industriels. pages 34–35, 2022. URL https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/.

[20] Stanislav Abaimov and Maurizio Martellini. Selected issues of cyber security practices in cbrnecy critical infrastructure. page 31, 2017.

[21] Vipin Kumar Aleksandar Lazarevic and Jaideep Srivastava. Intrusion detection: A survey. 2005. URL https://www.researchgate.net/publication/226650646_Intrusion_Detection_A_Survey.

[22] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, and Farhan Ahmad. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. 2020. URL https://onlinelibrary.wiley.com/doi/10.1002/ett.4150.

[23] Rebecca Bace and Peter Mell. Intrusion detection systems. 2001. URL https://search.worldcat.org/title/70689163.

[24] John R. Vacca. Managing information security. page 135, 2010.

[25] geeksforgeeks. Intrusion detection system (IDS), 2024. URL https://www.geeksforgeeks.org/intrusion-detection-system-ids/. accessed: 23-04-2024.