Improvement of smart grid stability **at times of network attacks using Artificial Intelligence**.

1. **Abstract:**

The power system worldwide is going through a revolutionary transformation due to the integration with various distributed components, including advanced metering infrastructure, communication infrastructure, distributed energy resources, and electric vehicles, to improve the reliability, energy efficiency, management, and security of the future power system. These components are becoming more tightly integrated with IoT. They are expected to generate a vast amount of data to support various applications in the smart grid, such as distributed energy management, generation forecasting, grid health monitoring, fault detection, home energy management, etc. With these new components and information, artificial intelligence techniques can be applied to automate and further improve the performance of the smart grid. As the smart grid involves various actors, such as energy produces, markets, and consumers, we also discuss how artificial intelligence and market liberalization can potentially help to increase the overall social welfare of the grid. As the smart grid involves various actors, such as energy produces, markets, and consumers, we also discuss how artificial intelligence and market liberalization can potentially help to increase the overall social welfare of the grid, Smart energy markets fascinated with artificial intelligence (AI) techniques can make it easier to design good policy incentives and allow consumers/utility to make decisions about their consumption/generation in an efficient way that contributes to the reduction of CO2 emissions. The challenges for AI in the electrical power system are designing automation technologies for heterogeneous devices that learn to adapt their consumption against pricing signals with user constraints, developing means of communication between humans and controllers, and designing simulation and prediction tools for consumers and suppliers

2. **Research Context**

As the energy sector is increasingly becoming complex, intelligent tools/mechanisms are needed to manage the system effectively and make timely decisions. In general, the artificial neural network (ANN), reinforcement learning (RL), genetic algorithm (GA), and multi-agent systems are well-known AI techniques to solve the problems of classification, forecasting, networking, optimization, and control strategies [4]. Due to the lack of advanced automatic controllable resources, many system operations are still performed manually or at a basic level of automation. However, the inclusion of AI in the grid system would introduce innovations and give new directions to the electrical grid

Optimization of controllable loads using intelligent techniques results in cost reduction. For example, Neves et al. [5] propose a genetic algorithm for the management of standalone microgrids (MGs) to optimize the controllable loads. With increases in computing power and

accessible data storage, AI techniques are offering much more efficient and powerful ways to handle the limitation of the traditional grid system. Besides, the application of distributed computing algorithms in SG has triggered many security issues. Physical and cyber attacks are the threats which can lead the infrastructure failure, privacy breach, disturbance, and denial of service (DoS) [6]. This paper reviews the current advances and challenges in the smart grid, distributed intelligence for future energy generation, and the role of distributed energy resources (DERs) in the future power system.

Artificial Intelligence in the Energy Industry

Any Artificial Intelligence is only as smart as its data. This is one of the biggest sticking points. The topics of **data protection and data security** are some of the greatest weak points for the use ofArtificialIntelligence.

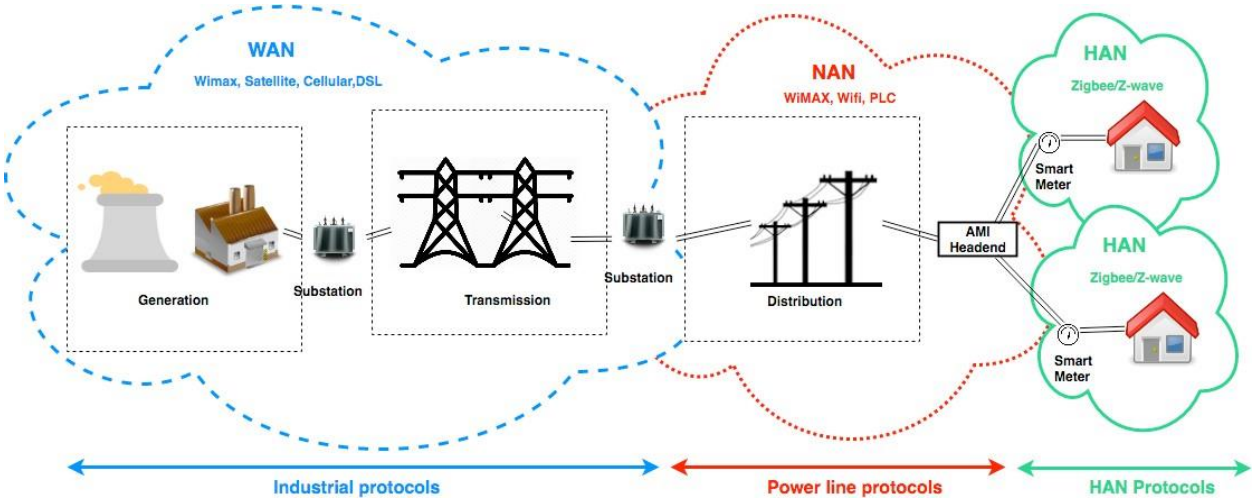
Those who are connected digitally and intelligently reveal a lot about themselves and the system becomes vulnerable to **cyberattacks**. In 2018, the German Federal Office for Security (BSI) observed that the number of cyberattacks on critical infrastructure tripled in comparison to the previous year. Energy supply and the entire energy system are part of this critical infrastructure. This is why cyber security is becoming more and more important today and in the future in order to protect the highly networked power grid from attacks and data theft from the outside. There are already strict security requirements for participants in the electricity market in the area of data protection and data security,though. Contrary to the widespread opinion that AI makes the power grid less secure, AI can make an important contribution in the fight against cyber attacks. It can quickly check large amounts of data and thus detect deviations. AI can also draw conclusions from past cyber attacks. Machine Learning has already achieved great success in this area, for example in the detection and defense of Trojans. Many end users are critical of Artificial Intelligence, especially in relation to smart home technologies. This is understandable, because the data of the most private space that reveals a lot about its users is collected. Studies have shown that the biggest obstacle to the acceptance of smart meters is fear of revealing private information without knowing exactly how it is used. These fears are justified, as there is still no regulation on how to handle this sensitive data, which is important for the electricity system of the future.Germany and the EU are trying to curb data access by private companies, as is happening in the USA and China, for example. The EU Commission has therefore developed four basic ethical principles for AIs: AI should respect human autonomy, avoid social harm, be fair, and be explainable. You can read these guidelines here. Especially the aspect of explainability will become more and more difficult with stronger and self-developing AIs.

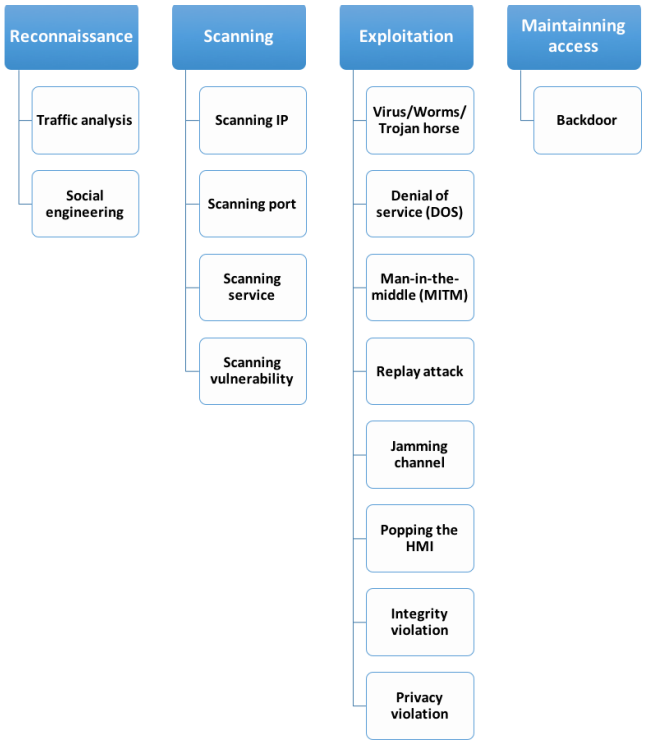
In order to give the energy industry and in particular end consumers more confidence in the AI, it must be clearly communicated how the data is used and by whom, and data security must be guaranteed.

Another criticism of AI is the **power consumption** of Artificial Intelligence itself. The processing of large amounts of data consumes a lot of electricity. When using AI for energy system transformation, it is crucial to analyze as well how to design the data centers themselves to be energy-efficient and as climate-neutral as possible. Possible solutions to this dilemma

include the physical proximity of data centers and renewable energy generation plants, the postponement of power-intensive computing operations to times when a lot of power is available, more energy-efficient IT hardware, or programming that requires as little computing power as possible.In the energy industry, AI offers a multitude of suitable application scenarios that will support the energy transition and a climate-friendly energy system. It will be crucial, however, to protect user data and make the use of AI transparent and comprehensible

Attacking cycle step	Attack category	Attack example	Compromised application/protocol in smart grid.	Compromised security's parameter	Possible countermeasures
Reconnaissance	Traffic analysis	[33]	Modbus protocol, DNP3 protocol	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK), TLS, SSL, Encryption, Authentication[1, 7]
	Social engineering	Phishing [29]			
		Password pilfering [30]			
Scanning	Scanning IP, Port, Service, Vulnerabilities	Modbus network scanning [25]	Modbus Protocol	Confidentiality	IDS, SIEM, Automated[1] security compliance checks [48]
		DNP3 network scanning [24]	DNP3 Protocol		
Exploitation	Virus, worms, Trojan horse	Stuxnet [8]	SCADA PMU, Control device	Confidentiality Integrity Availability Accountability	DLP , IDS , SIEM, Anti-virus [1], Diversity technique[49]
		Duqu [8]	SCADA		
	Denial of service (DOS)	Puppet attack [15]	AMI	Availability	SIEM, IDS [1], flow entropy, signal strength, sensing time measurement, transmission failure count, pushback, reconfiguration methods [4, 44]
		TDS [34]	Instability of smart grid systems		
		TSA [35]	PMU, smart grid equipment's GPS		
	Man-in-the-middle (MITM)	eavesdropping attack [1, 33]	HMI, PLC	Confidentiality Integrity	Secure DNP3, PKI (SKMA, SMOCK) [7], TLS, SSL, encryption, authentication [1]
		[17]	SCADA		
		[36]	DNP3, SCADA		
		Intercept/alter [33]	AMI		
	Replay attack	[1]	IED, SCADA, PLC	Confidentiality Integrity	Secure DNP3, TLS, SSL, encryption, authentication[1] PKI (SKMA, SMOCK) [7],
		[33]	Authentication scheme in AMI		
	Jamming channel	[38]	PMU	Availability	JADE, anti-jamming (FHSS, DSSS) [38]
		MAS-SJ [16]	CRN in WSGN		
	Popping the HMI	[1]	SCADA, EMS, substations.	Confidentiality Integrity Availability Accountability	DLP, IDS , SIEM , Anti-virus [1], automated security compliance checks [48]
	Masquerade attack	[33]	PLC	Confidentiality Integrity Availability Accountability	DLP, IDS, Secure DNP3, SIEM, TLS, SSL, encryption, authentication [1], PKI (SKMA, SMOCK)[7]
	Integrity violation	[1]	Smart meter, RTU	Integrity Availability	DLP, IDS ,SIEM, Secure DNP3, TLS, SSL, encryption, authentication [1], PKI (SKMA, SMOCK) [7, 45]
		FDI [40], [41]	EMS, SCADA, AMI		
	Privacy violation	[28], [42]	Demand Response program, Smart meters.	Confidentiality	Secure DNP3, PKI (SKMA, SMOCK)[7], TLS, SSL, encryption, authentication [1]
Maintaining access	Backdoor	[43]	SCADA	Confidentiality Integrity Availability Accountability	IDS, SIEM,Anti-virus [1], Diversity technique[49]


WAN
Wimax, Satellite, Cellular,DSL
NAN
WiMAX, Wifi, PLC
HAN
Zigbee/Z-wave
Smart Meter
HAN
Zigbee/Z-wave
Smart Meter
AMI Headend
Generation
Substation
Transmission
Substation
Distribution
Industrial protocols
Power line protocols
HAN Protocols


Reconnaissance
Traffic analysis
Social engineering
Scanning
Scanning IP
Scanning port
Scanning service
Scanning vulnerability
Exploitation
Virus/Worms/ Trojan horse
Denial of service (DOS)
Man-in-the-middle (MITM)
Replay attack
Jamming channel
Popping the HMI
Integrity violation
Privacy violation
Maintainning access
Backdoor