

Artificial Intelligence and Cyber Security: Protecting and Maintaining Industry 4.0 Power Networks

Sahli Nabil^a, Benmohammed Mohamed^b, Hugues Bersini^c and El-Bay Bourenane^d

^aSADEG- RDE SONEGGAZ, Algeria & LIRE Laboratory Constantine 2 University, Algeria
nabil.sahli@etu-univ-amu.fr and sahli.nabil@rde.sadeg.dz

^bLIRE Laboratory Constantine 2 University, Algeria
mohamed.benmohammed@univ-constantine2.dz

^cIRIDIA Laboratory ULB University, Bruxelles, Belgium
hugues.bersini@ulb.ac.be

^dLE2I Laboratory UBFC University, Dijon, France
ebourenn@u-bourgogne.fr

Abstract

This survey paper describes a literature review of machine learning and deep learning (DL) methods for AI cyber security applications. A short tutorial-style description of each artificial intelligence and data meaning method are provided, including deep learning, restricted Boltzmann machines, Feed forward deep neural network, recurrent neural network, deep belief network, deep auto-encoder, deep migration learning, self-taught Learning and replicator neural network. Then we discuss how each of the DL methods is used for security applications for SCADA systems and smart grids. We conclude that artificial intelligence in cyber Security challenges to adopt DL.

Keywords

Cyber Security ; machine Learning ; AI secure bloc ; Smart Grid security.

IAM'20: The 3rd Conference on Informatics and Applied Mathematics, October 21–22, 2020, LabSTIC Guelma University Algeria.



© 2020 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).



CEUR Workshop Proceedings (CEUR-WS.org)

1. Introduction

Critical National Infrastructures (CNIs) such as ports, water and gas distributors, hospitals, energy providers are becoming the main targets of cyber-attacks. (Supervisory Control and Data Acquisitions -SCADA) or Industrial Control Systems (ICS) in general are the core systems that CNIs rely on in order to manage their production.

The Algerian industrial group SONELGAZ relies on its research and development and its capacity to innovate to ensure its public service missions in an ever more efficient way by inventing the electrical network as well as the security and maintenance solutions of tomorrow, it will be more "Smart", more digital, more automatic and more interactive, serving customers, players in the electricity market and the development of smart cities. The research and innovation program contributes to the digital transformation of the company and to the proactive support of the energy transition to renewable energies. Mainly composed of applied research activities, experimental development and supplemented by an "Open Innovation" device to establish collaborations with promising research and innovation startup companies, the research and development program is enriched by experiments carried out in demonstrators and on real equipment.

The electricity transmission or distribution system operator must always seek the best balance between investment and maintenance policies for electrical works, component performance, level of network automation and optimization of tools. "SCADA" driving experience. The SONELGAZ group is also investing in research to have innovative or communicating components, develop the automation of electrical networks and modernize driving tools (information system and SCADA). The objective is in particular to increase the observability and piloting capacities from the driving rooms for better management of electrical constraints, in advance and in real time.

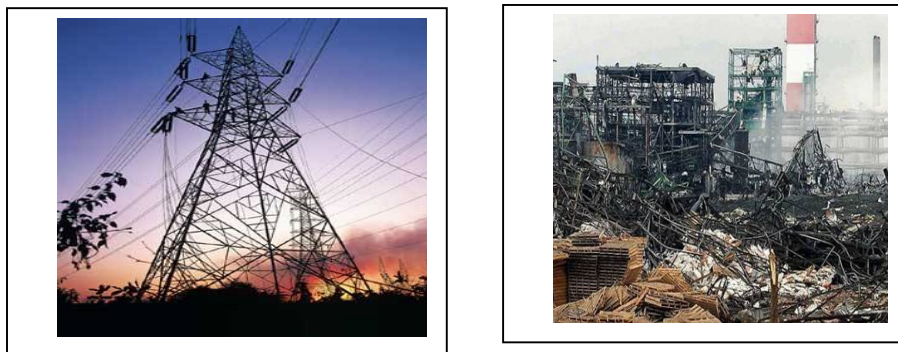


Figure 1: Cybersecurity AI for Industry 4.0 Smart Grids [1]

We review the cyber security IA for industry 4.0 smart systems that use deep learning approaches. We present the smart grid security for electricity transport and distribution. We analyze seven deep learning approaches according to two models, namely, deep discriminative models and (generative/unsupervised) models. The deep discriminative models include three approaches:

- Recurrent neural networks, (ii) deep neural networks, and (iii) convolutional neural networks.
- The generative/unsupervised models include four approaches: (i) deep auto encoders, (ii) restricted Boltzmann machine, and (iii) deep Boltzmann machines, and (iv) deep belief networks.

The Mediterranean electric loop is an example of interconnected smart electricity networks. With exchanges between SCADA systems (international emergency alarms). A Mediterranean market for the marketing of electricity is developing as well as energy support between countries to avoid "Blackouts", as presented in Figure 2.

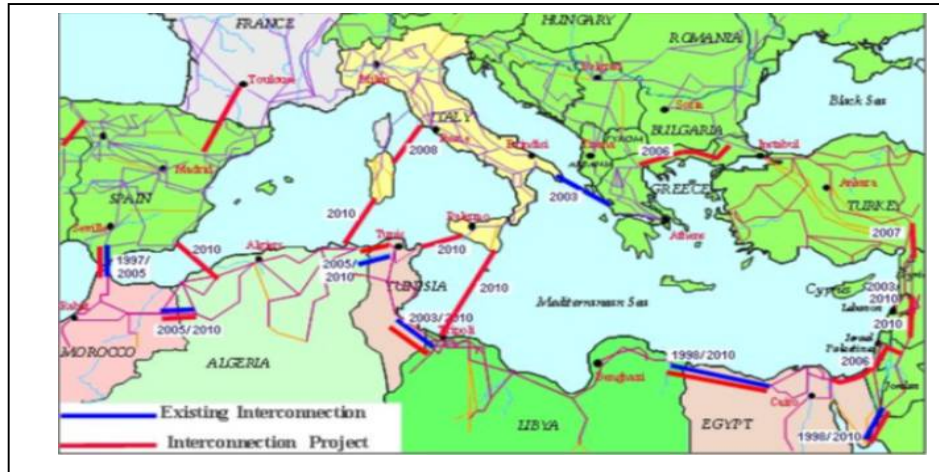


Figure 2: Interconnected electrical networks for marketing and energy security needs [2]

2. Similar work

In the literature, there are different related studies that deal with machine learning techniques for industry 4.0 cyber security; we categorize the studies based on the following criteria:

- Deep learning approaches: it specifies if the study was focused on Deep learning approaches for industry 4.0 smart systems cyber security [3].
- Machine learning approaches: it indicates whether the study considered machine-learning approaches for industry 4.0 smart systems cyber security [4, 5].
- Evaluation of deep learning approaches: it indicates whether the study evaluates deep learning approaches for industry 4.0 smart systems cyber security [6].
- Evaluation of machine learning approaches: it indicates whether the study evaluates machine-learning approaches for industry 4.0 smart systems cyber security [7].

Study	Year	DL	ML and DM	EDL	EML
Buczak et al. [8]	2015	No	Yes	No	No
Milenkoski et al. [9]	2015	No	Partial	No	Partial
Folino et al. [10]	2016	No	Yes	No	No
Zarpelao et al. [11]	2017	No	Partial	No	No
Aburomman and Reaz [12]	2017	No	Yes	No	Partial
Xin et al. [13]	2018	Yes	Partial	No	No
Ring et al. [14]	2019	No	No	No	No
Loukas et al. [15]	2019	No	No	No	No
Costa et al. [16]	2019	No	No	No	No

Chaabouni et al. [17]	2019	Partial	Yes	No	Partial
Berman et al. [18]	2019	Yes	Partial	No	No
Mahdavifar et al. [19]	2019	Yes	Partial	No	No
Sultana et al. [20]	2019	No	Yes	No	No
Our Study	2020	Yes	Partial	Yes	Partial

ML and DM: Machine learning (ML) and data mining (DM) approaches; DL: Deep learning approaches; EDL: Evaluation of deep learning approaches; EML: Evaluation of machine learning approaches.

3. The motivations of our research work

3.1. Drones for the maintenance of overhead electrical networks

Drones, associated with increasingly efficient optical sensors, can facilitate the maintenance of aerial electrical works. To punctually inspect electrical works that are difficult to access from the ground and improve the diagnosis on the state of the components (concept of the remote eye). The ultimate goal would be to be able to use them for line visits over long distances: detection of defective equipment, inventory of vegetation near the works to prioritize pruning. In line with its contribution to the work of the Council for Civil drones presented in Figure 3, steered by the Directorate General of Civil Aviation, the SONELGAZ group will launch several experiments. One of them aims to carry out a vegetation survey by photogrammetry. The group is also involved in a consortium on the design of a LIDAR type sensor, which can be integrated into drones for operations over long distances; also manage all the components of the intelligent electrical network in a centralized and cyber secure manner.



Figure 3: Drone for electrical grid maintenance

3.2. Project for the modernization of remote control systems (SCADA)

The project (Intelligence Control-Command Driving) aims to modernize the SONELGAZ group's Remote-control systems, by exploiting existing business objects and new Smart objects in an industrial and evolutionary way, all along the chain, from the Agency of Conduct

to the (MV / LV) public distribution stations via the source stations. This is reflected in the development of an interoperable system (standard 61850) allowing centralized and cyber secure management of all the Smart objects that can be deployed on the network (Management System): remote administration, remote configuration and supervision. The work has advanced significantly with in particular the specification of the local Management System of (HTB / HTA) stations (PCCN) and the prototyping of the new digital and cyber-secure device and of exchange of information in operation with producers connected in HTA.

3.3. Objects connected to the operation of the electricity network

For the SONELGAZ group, the development of communicating objects and low-cost communication networks suggests potential contributions for the operation of the distribution network as presented in Figure 4. In collaboration with the ecosystem of startups, SONELGAZ plans to experiment with various emerging objects in order to continue to improve the quality of service for network users. It is a question of quickly testing the potential value of different objects for the businesses of the SONELGAZ group, and in case of demonstrated value, of planning their integration on a large scale. He also developed a secure tool to manage these objects and associated data, and make them available to the professions concerned. Also an integrated CRMS for the management of its clientele and the entire commercial chain.

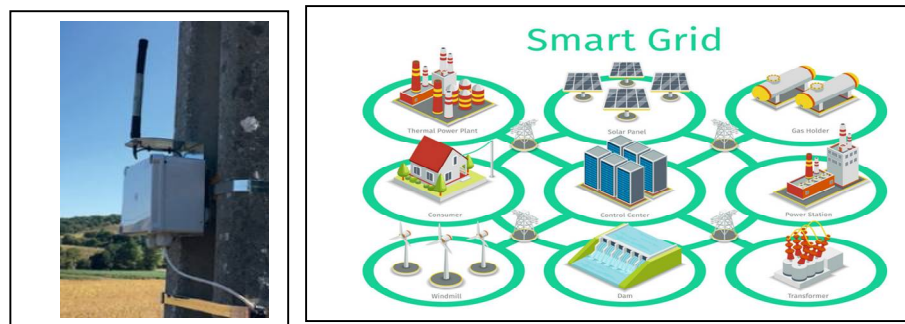


Figure 4: Monitoring of electricity smart grids by wireless sensors at SONELGAZ.

3.4. Cyber security of energy information systems in Algeria

With the increase in data exchanges between the various Information Systems, the control of cybersecurity issues becomes more and more critical, in particular for remote control and SCADA systems, hitherto very closed, even then that the number of cyber-attacks recorded on industrial is growing exponentially, in particular in the field of electric and gas energy. As part of the project (Intelligence Control-Command Driving), a (PoC - Proof of Concept) of the cyber-secure tele-driving channel was carried out. The Management System for Connected Objects has been the subject of specific considerations in terms of the engineering of connected objects and the processes for monitoring operational exchanges between these same objects.

3.5. Big Data processing for massive data management (SCADA and contact center)

The SOBELGAZ group has developed an IT infrastructure based on a Big Data architecture to perform more sophisticated and faster data processing. These capacities are in particular tested for the massive processing of metering data in the field of flow reconstruction, at the

service of the various Balance Managers. In addition, the SONELGAZ group is strengthening its role as a data operator by making consumption data available to the general public via its Open Data portal, and by developing an API (Application Programming Interface) platform with a view to expose data to customers (invoices, complaints, connection requests, etc.) market players while ensuring their protection, also setting up contact centers "call centers" with the toll-free call number for real-time management of customer relations as well as the collection of a large mass of data which requires cyber security solutions based on artificial intelligence, to deal with future cyber-attacks which will also be based on artificial intelligence.

3.6. Facilitate the integration of electric vehicles and the emergence of Smart Cities

The SONELGAZ group must indeed prepare to support the development of smart cities or districts, positive energy territories, positive energy buildings and local energy communities. The SONELGAZ group is also widely involved in actions to accommodate charging facilities, conditions necessary for the development of the electric vehicle (EV) they are planned at the East-West motorway primarily in Algeria. The challenges are for the SONELGAZ group to optimize the volume of investments to strengthen the electricity network, to control the impact of charging infrastructure on the quality of the electricity supplied and to facilitate the implementation of new business models. "Business models" introduced by the development of electric vehicles (roaming and other mobility services). Cybersecurity based on artificial intelligence and at the center of interest for the integration of electric vehicles and the emergence of smart cities. One of the SONELGAZ group's smart management of electric vehicle charging has developed algorithms for smart charging management. These algorithms make it possible to control the power calls linked to EV charging and to consume outside carbon production peaks, while satisfying the driving needs of the next day.

4. The art state

The research and development theme aims to enable the SONELGAZ group to facilitate developments in the electrical system and to contribute to the energy transition to renewable energies, which involves preparing for developments in the profession of the distributor and transporter of electrical energy to the management of the smart electricity networks of tomorrow and the management of the data operator mission for the benefit of external actors. The future model of industrial 4.0's electrical networks is presented in Figure 5.

Industry 4.0 components are cyber physical systems, internet of things, smart factory, web services, smart product, machine-to-machine, big data, Cloud, robots and smart embedded systems. Industry 4.0 model implemented in Critical infrastructure, supervision and control of electricity smart grid, oil and gas transport and distribution networks. Industry 4.0 design principles technologies we used are synthetized in Figure 6.

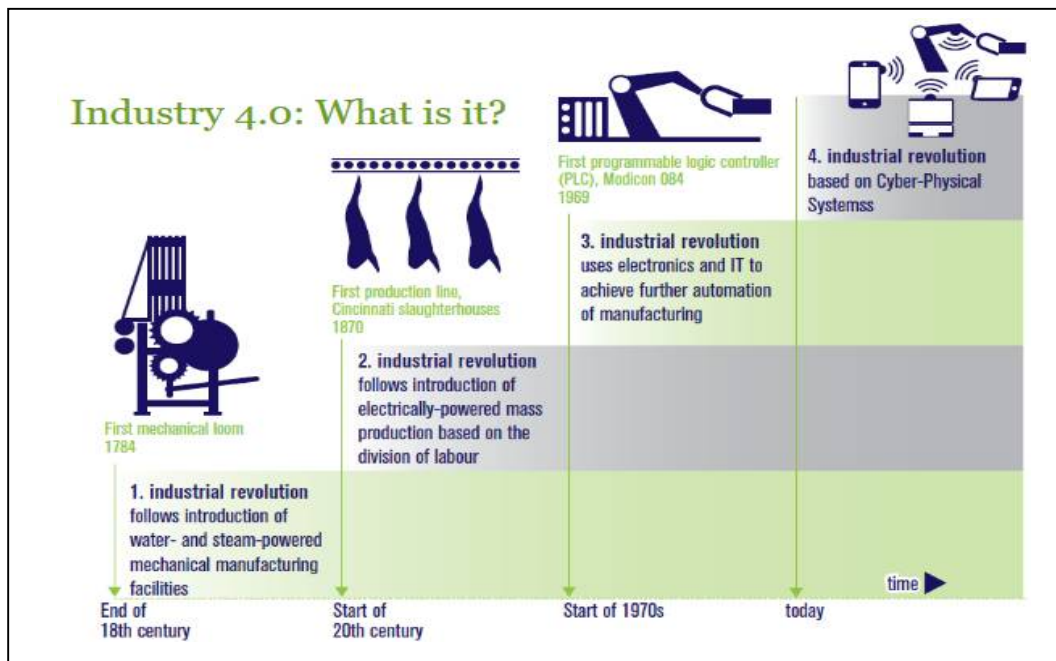


Figure 5: Industry 4.0 model.

	Cyber-Physical Systems	Internet of Things	Internet of Services	Smart Factory
Interoperability	X	X	X	X
Virtualization	X	-	-	X
Decentralization	X	-	-	X
Real-Time Capability	-	-	-	X
Service Orientation	-	-	X	-
Modularity	-	-	X	-

Figure 6: Industry 4.0 design principles technologies

From Industry 4.0 to Energy 4.0, industry in general has recognized that we are at the beginning of a revolution that is fundamentally changing the way we live, work, and relate to one another, energy has been key to all industrial revolution so far, the energy industry may not have fully realized how much the current industrial revolution will be transforming the energy industry. At a time, when the energy industry is struggling with the Energy wend. At a time, when other industries are already in the process of realizing what potential and what risk are associated with Industry 4.0 (big data, artificial intelligence, cyber security attacks, semantic and ontologies, cloud and IoT).

The integration of intermittent renewable energies, the development of active demand management, electric vehicles and decentralized storage require an evolution in the role of the

distributor. The SONELGAZ group carries out R&D actions to facilitate the transformations of the electrical system, the development of markets and the integration of producers on the distribution network, while maintaining the quality of supply and the cyber security of the functioning of the smart grid in the context of industry 4.0.

5. Our proposed energy 4.0 and business model

Digitization of the energy industry will be a key driver of future change; the energy industry will have to look to the IT and telecommunications industry and other advanced industries for technical, commercial and legal experience. Energy lawyers will need to better understand legal problems and solutions those other industries can offer. No need to reinvent the wheel, but have to make wheel work in a heavy duty, high speed scenario, with many quick turns, in often uncharted territory, as presented in Figure 7.

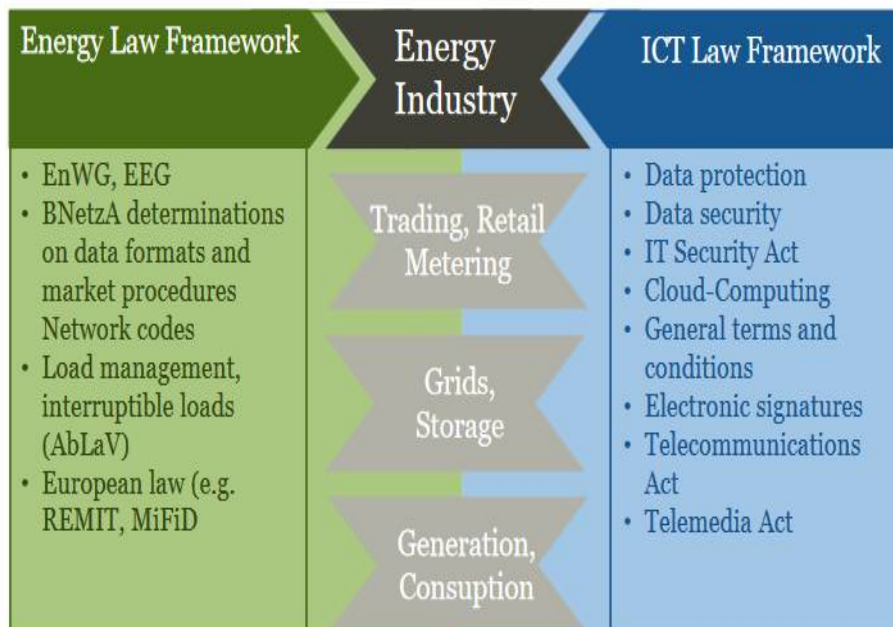


Figure 7: Our proposed energy 4.0 and business models for industry 4.0 at SONELGAZ.

6. The current situation of cyber security

The current cyber security domain of systems presents a missing link, which is the use of artificial intelligence, as dynamic self-learning methods to respond to new threats, and this following the future use of hackers. Techniques based on artificial intelligence for their attacks on industry 4.0 systems. The weak link in cyber security chain for industry 4.0 presented in Figure 8.

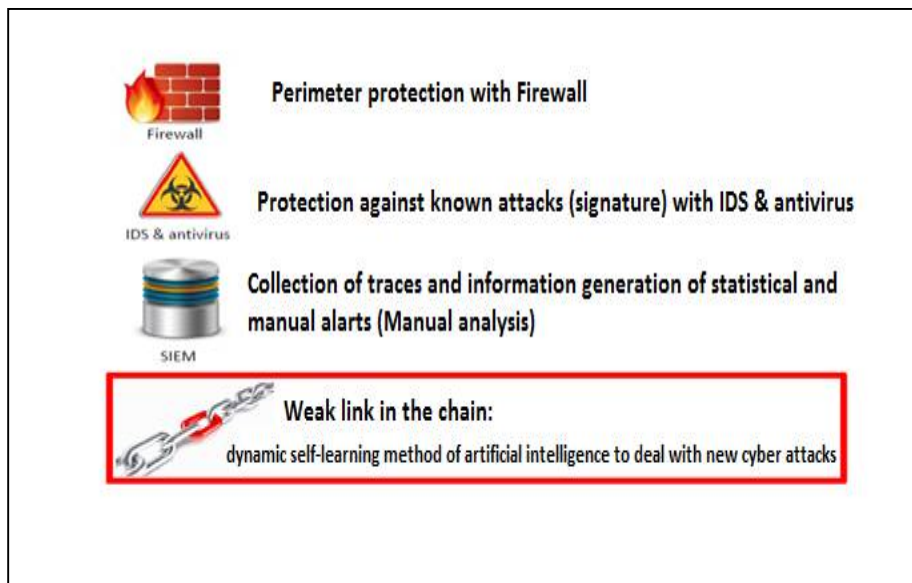


Figure 8: The weak link in cyber security chain for industry 4.0.

(Intrusion detection systems - IDS) [2], is part of the second defense line of a system. IDS can be deployed along with other security measures, such as access control, authentication mechanisms and encryption techniques in order to better secure the systems against cyber-attacks. Using patterns of benign traffic or normal behavior or specific rules that describe a specific attack, IDSs can distinguish between normal and malicious actions [3].

7. Artificial intelligence evolution and our choices for secure industry 4.0

The evolution of artificial intelligence is summed up in Figure 9. We propose in our works the use of deep learning to secure smart systems and communications in the industry 4.0 control systems as smart grid used in the electricity transport and distribution industry in SONELGAZ group.

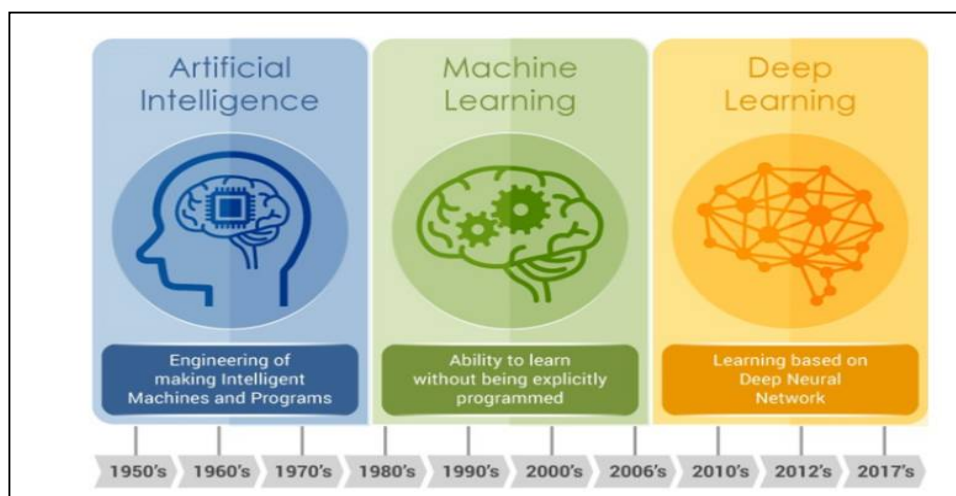


Figure 9: Artificial intelligence evolution and definitions [21].

Also known as deep learning is a sub-domain of machine learning, which involves the processing by computers of large amounts of data using artificial neural networks whose structure mimics that of the human brain. Whenever new information is integrated, the existing connections between neurons are susceptible to modification and extension, which has the effect of allowing the system to learn things without human intervention, independently, while improving the quality of its decision-making and forecasting. Our secure Deep learning model for SCADA systems secure bloc detail is presented in Figure 10.

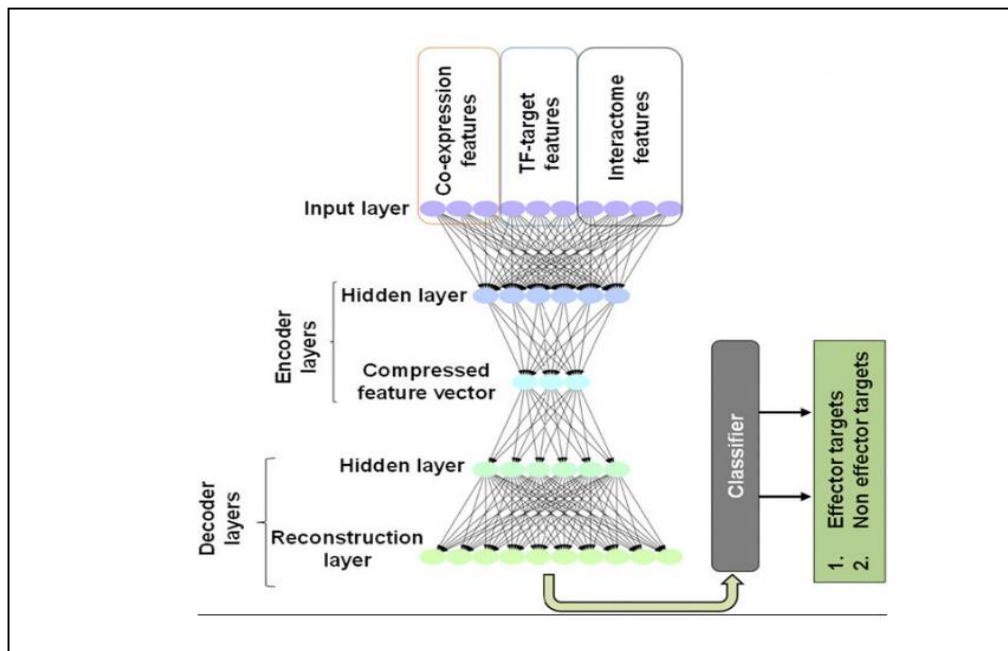


Figure 10: Deep learning layers and mechanism proposed for AI secure bloc.

8 Our theory contributions

Our contributions in this work are presented below composed the AI secure bloc:

- We review the future Firewall that use deep learning approaches, we named Firewall AI.
- We review the intrusion detection systems that use deep learning approaches in IDS AI.
- We review the future antivirus that use deep learning approaches, we named antivirus AI.
- We analyze seven deep learning approaches according to two models, namely, deep discriminative models and (generative/unsupervised) models. The deep discriminative models include three approaches:

(i) Recurrent neural networks, (ii) deep neural networks, and (iii) convolutional neural networks. The generative/unsupervised models include four approaches: (i) deep auto encoders, (ii) restricted Boltzmann machine, and (iii) deep Boltzmann machines, and (iv) deep belief networks.

- We compare the performance of deep learning approaches with four machine learning approaches, namely, Naive Bayes, Artificial neural network, Support Vector Machine, and Random forests.

We proposed the future electricity secure AI model proposed for industry 4.0 as presented in Figure 11 and Figure 12.

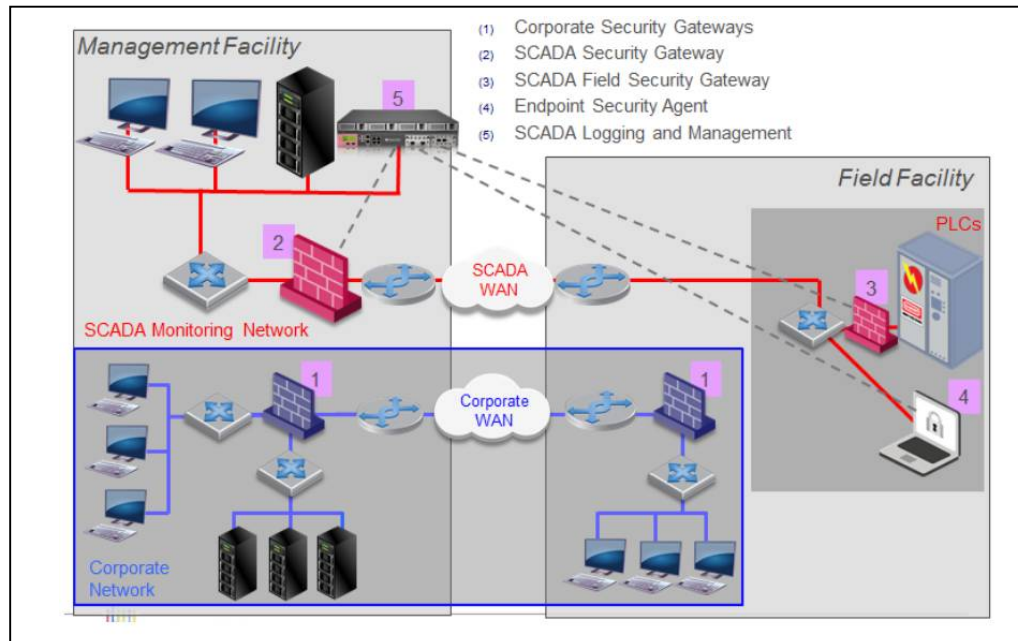


Figure 11: Future secure AI electricity (MDE- Model Driven Engineering) model proposed.

Cyber-attacks using the Internet. Machine learning (ML) and artificial intelligence techniques have been widely used to constitute an intelligent and efficient Intrusion Detection System dedicated to ICS. Generally develop and train their ML-based security system using network traces obtained from publicly available datasets. Due to malware evolution and changes in the attack strategies, these datasets fail to protect the system from new types of attacks, and consequently, the benchmark datasets should be updated periodically.

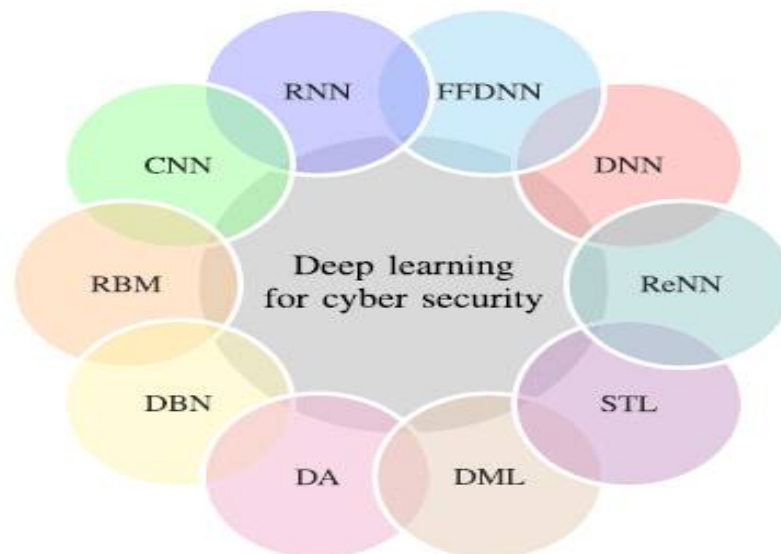


Figure 12: Deep learning approaches used for industry 4.0-cyber security IA proposed

Deep learning approaches we used for industry 4.0 cyber security IA are (FFDNN: Feed forward deep neural network); (CNN: Convolutional neural network); (DNN: Deep neural network); (RNN: Recurrent neural network); (DBN: Deep belief network); (RBM: Restricted Boltzmann machine); (DA: Deep auto-encoder); (DML: Deep migration learning); (STL: Self-Taught Learning) and (ReNN: Replicator Neural Network).

9 Conclusion

This paper presents the deployment of a SCADA system at SONELGAZ group Algeria in the context of interconnected Mediterranean smart grids, for cybersecurity research and investigates the feasibility of using ML algorithms to detect cyber-attacks in real time. The SONELGAZ SCADA was built using equipment deployed in real industrial settings. Sophisticated attacks were conducted on to develop a better understanding of the attacks and their consequences in SCADA and smart grid environments.

We conducted a comparative study of deep learning approaches for cyber security AI, we used for secure AI industry 4.0 smart systems, namely, deep discriminative models and (generative/unsupervised models. Specifically, we analyzed seven deep learning approaches, including recurrent neural networks, deep neural networks, restricted Boltzmann machine, deep belief networks, convolutional neural networks, deep Boltzmann machines, and deep auto encoders.

Acknowledgments

Thanks to IRIDIA ULB Belgium university, LE2I UBFC university France and LIRE Constantine 2 university Algeria that assisted in the research and the preparation of the work with SONELGAZ group Algeria.

References

- [1] L.A. Maglaras, K.-H. Kim, H. Janicke, M.A. Ferrag, S. Rallis, P. Fragkou, et al.: Cyber security of critical infrastructures ICT Express, 4 (1), pp. 42-45, (2018).
- [2] A. Ahmim, M. Derdour, M.A. Ferrag: An intrusion detection system based on combining probability predictions of a tree of classifiers Int. J. Commun. Syst., 31 (9), pp. 35-47, (2018).
- [3] A. Ahmim, L. Maglaras, M.A. Ferrag, M. Derdour, H. Janicke: A novel hierarchical intrusion detection system based on decision tree and rules-based models 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE, pp. 228-233, (2019).
<https://ieeexplore.ieee.org/abstract/document/8804816/>
- [4] Z. Dewa, L.A. Maglaras: Data mining and intrusion detection systems, Int. J. Adv. Comput. Sci. Appl., 7 (1), pp. 62-71, (2016).
- [5] B. Stewart, L. Rosa, L.A. Maglaras, T.J. Cruz, M.A. Ferrag, P. Simões, et al: A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes. EAI Endorsed Trans. Ind. Netw. Intell. Syst., 4 (10), p. 4, (2017).
- [6] I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani: Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSP, pp. 108-116, (2018).
- [7] M.A. Ferrag, L. Maglaras, H. Janicke, R. Smith: Deep learning techniques for cyber security intrusion detection: a detailed analysis 6th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2019), Athens, 10–12 September, (2019).
- [8] A.L. Buczak, E. Guven: A survey of data mining and machine learning methods for cyber security intrusion detection IEEE Commun. Surv. Tut, 18 (2), pp. 1153-1176, (2015).

- [9] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer: Payne Evaluating computer intrusion detection systems: a survey of common practices ACM Comput. Surv, 48 (1) (2015), p. 12, (2015).
- [10] G. Folino, P. Sabatino Ensemble based collaborative and distributed intrusion detection systems: a survey J. Netw. Comput. Appl., 66, pp. 1-16, (2016).
- [11] B.B. Zarpelao, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga: A survey of intrusion detection in internet of things J. Netw. Comput. Appl., 84, pp. 25-37, (2017).
- [12] A.A. Aburomman, M.B.I. Reza A survey of intrusion detection systems based on ensemble and hybrid classifiers Comput. Security, 65, pp. 135-152, (2017).
- [13] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, et al. Machine learning and deep learning methods for cybersecurity IEEE Access, 6 , pp. 35365-35381, (2018).
- [14] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho A survey of network-based intrusion detection data sets Comput. Security, (2019).
- [15] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, T. Vuong A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles Ad Hoc Netw., 84 , pp. 124-147, (2019).
- [16] K.A. da Costa, J.P. Papa, C.O. Lisboa, R. Munoz, V.H.C. de Albuquerque Internet of things: a survey on machine learning-based intrusion detection approaches Comput. Netw., 151 (2019), pp. 147-157, (2019).
- [17] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki: Network intrusion detection for IoT security based on learning techniques IEEE Commun. Survey. Tut, (2019).
- [18] D.S. Berman, A.L. Buczak, J.S. Chavis, C.L. Corbett: A survey of deep learning methods for cyber security. Information, 10 (4), p. 122, (2019).
- [19] S. MahdaviFar, A.A. Ghorbani Application of deep learning to cybersecurity: a survey Neuro computing, (2019).
- [20] N. Sultana, N. Chilamkurti, W. Peng, R. Alhadad Survey on SDN based network intrusion detection system using machine learning approaches Peer-to-Peer Netw. Appl., 12 (2), pp. 493-501, (2019).
- [21] T. Salman, D. Bhamare, A. Erbad, R. Jain, M. Samaka. Machine learning for anomaly detection and categorization in multi-cloud environments. In Proceedings of the 4th IEEE International Conference on Cyber Security and Cloud Computing, New York, NY, USA, 26–28 June, (2017).