Proceedings of the 20th Conference on Computer Science and Intelligence Systems (FedCSIS) pp. 771–776
DOI: 10.15439/2025F0792
ISSN 2300-5963 ACSIS, Vol. 43

AI Software Security for Smart Environment in a Dynamically Changing Knowledge Management Strategy

Anna Sołtysik-Piorunkiewicz
0000-0002-7935-1377
University of Economics in Katowice
ul. 1 Maja 50, 40-287
Katowice, Poland
Email: anna.soltysik-piorunkiewicz@uekat.pl

Małgorzata Pańkowska
0000-0001-8660-606X
University of Economics in Katowice
ul. 1 Maja 50,
40-287 Katowice, Poland
Email: malgorzata.pankowska@uekat.pl

Stanisław Stanek
0000-0001-9939-4350
Emeritus of General Tadeusz Kościuszko Military University of Land Forces,
Wrocław, Poland
Email: swstanek@gmail.com

Karsten Böhm
0000-0002-2950-7433
FH Kufstein Tirol
Andreas Hofer Str. 7
6330 Kufstein, Austria
Email: karsten.boehm@fh-kufstein.ac.at

Mariusz Żytniewski
0000-0003-2170-1191
University of Economics in Katowice
ul. 1 Maja 50,
40-287 Katowice, Poland
Email: zyto@ue.katowice.pl

***Abstract*—The theory of smart environments assumes a diversity of human-supporting solutions that interact with each other and are oriented towards applying artificial intelligence. Concepts such as digital twin, software agent, and machine learning can aid the creation of smart environments by supporting the design and simulation of device behaviors. This article aimed to conduct research addressing the question how does multi-agent software impact smart grid security and show the practical exemplification of supporting smart grid security with multi-agents system. The paper's research findings discussed the AI-based knowledge management model in the context of the GRAI framework usage, which stands for Generative, Receptive Artificial Intelligence, and presents a proposal of an updated model that takes into account recent developments regarding GenAI and its consequences for KM. Based on the conducted research, an algorithm for collecting information from devices was proposed and used in a simulation based on the Isolation Forest algorithm.**

***Index Terms*—Digital Twin, Smart Grid, Internet of Things, Internet of Intelligence, Immersive Technology, Smart Environment**

I. Introduction

THE development of the Internet of Things (IoT) [5], and Internet of Intelligence (IoI) theory [26] points to a wide range of smart solutions in everyday life. Concepts such as smart city, smart home, smart grids, and others allow for the application of information solutions in user support and provide the capability to process large amounts of data. In the context of smart systems, perceiving them as distributed architecture systems requires appropriate management, monitoring, and security. Smart environments can encompass a variety of smart solutions, including smart grids, smart homes, and smart cities. The melding of these solutions is an important area of research. Exploring ways to integrate them represents a key direction in the development of smart-environment theory.

Smart environments refer to the multiple application domains where real-time Internet of Things (IoT) data processing allows for improved decision-making. These are ecosystems in which humans, conventional computer systems, and IoT devices are combined through cyber-physical services. Smart environments represent any physical environment augmented with a collection of embedded systems elaborating heterogeneous data and interacting with people.

Typically, smart cities aim at providing applications such as smart transportation, smart grids, smart surveillance, to enhance urban living standards by IoT, AI, digital twins, augmented reality, and the metaverse. A smart city typically comprises smart homes, smart health, smart roads, smart parking, and smart people. Similarly, smart health spaces like smart hospitals, smart gyms, or smart retirement homes are aimed at continuous patient monitoring and therapy provision. The term smart home is used to describe homes with home applications, illumination, heating, air conditioning, television, computers, audio and video entertainment systems, security systems, and camera schemes. Smart building is to monitor the energy and water utilization, as well as emissions and waste products. A smart environment can be made up of users' wearable and handheld devices, and several smart personal spaces. Smart agriculture assists farmers in minimizing wastage and improving productivity because the systems support irrigation and crop field monitoring. A smart traffic light

system can monitor green light times and automatically switch lights to avoid traffic jams. Smart environments encompass a large set of technologies, including computer networking, wireless communication, computational infrastructures, sensor networks, and algorithm design (Fig 1).

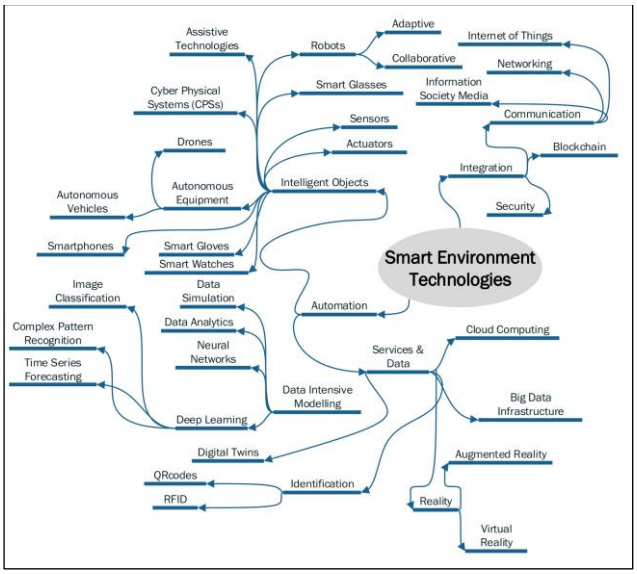

Fig 1. Smart environment technologies

The critical outcome of smart environment applications and execution is the generation of large-scale data sets. This large amount of data requires significant processing through artificial intelligence and machine learning algorithms. The term ‘smart’ was originally an acronym standing for “Self-Monitoring, Analysis and Reporting Technology”, but smart technology is now defined as much by its capacity to monitor and track its user activities, preferences, and regularities [29].

In this paper, the impact of multi-agents on the smart grid is detailed by the assumptions of smart grid security, adaptability, and user-friendliness factors. The following research questions were formulated:

- RQ1: How does multi-agent software impact smart grid security?
- RQ2: How to implement the multi-agent in a smart environment with current AI software?

The theoretical background was presented in Section 2. The research began with a preliminary study of the literature review, which is presented in Section 3. The empirical part of the study will demonstrate how a multi-agent system can be applied to enhance the security of a home grid network. The practical exemplification of the usage of multi-agent software was presented in Section 4.

The topic presented here is becoming increasingly actual and relevant in dynamically changing environments with its threats, which are related to, e.g., climate change, the energy crisis, or limited resources. The presented findings are an itemization of the factors that might be useful for further work, academic researchers, or business practitioners.

II. Theoretical Background

A. Multi-Agents software implementation

The areas of the Smart Environment theory, which include the smart grid theories discussed here, require the analysis of many aspects in the design and construction of modern computer systems. As the authors indicate [26], the Internet of Intelligence (IoI) requires defining the research area, the technologies in which the solution is being developed, its architecture, and identifying research gaps. Based on the research methodology, the studies undertaken in the article relate to Smart Grid/Energy in terms of application areas, Artificial Intelligence, Digital Twin, Immersive Technology in terms of considered technologies, and Modeling Intelligence and Security and Privacy in terms of the defined gaps in research discussed in the article.

From a technological perspective, the research considerations have been focused on multi-agent systems, which allow for the creation of intelligent and autonomous systems. These have the ability not only to automate processes but also to act on behalf of users within information systems in the context of Digital Twin (DT) theory. The use of multi-agent systems in the context of the Internet of Intelligence allows for a range of benefits such as the implementation of well-defined communication standards between agents and the creation of a system architecture within the framework of DT theory.

The features of multi-agent systems presented here suggest various possible scenarios for using these systems during the development of Internet of Intelligence systems.

B. Smart grid systems and security

One of the areas of implementing the IoI theory is smart grid systems. A smart grid (SG), also called smart electrical/power grid, intelligent grid, intelligrid, future grid, intergrid, or intragrid, is an enhancement of the 20th-century power grid. The traditional power grids are generally used to carry power from a few central generators to a large number of users or customers. In contrast, the SG uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network.

Due to the importance of the energy sector for the safety and uninterrupted operation of systems and devices, the search for solutions that safeguard such systems is a very important element in the development of IoI theory.

The Smart Grid term encapsulates the convergence of remote monitoring and control technologies with communication technologies, renewable generation, and analytics capabilities so that electric, natural gas, and water grid infrastructures can continuously provide information for operational and strategic management. The smart grids’ security challenges cover assurance of reliability and resilience of energy supply power, as well as safety, possible expansion and improvement plans, and efficiency of energy provision [2].

The ISO standards on smart grid security are as follows: ISO/IEC DIS 27019 Information technology Security techniques, Information security controls for the energy utility industry [38], ISO/IEC 30101:2014 Information technology,

Sensor networks: Sensor network and its interfaces for smart grid system [39].

C. Multi-Agent software in smart-grid system implementation

Within the framework of IoI theory, it becomes necessary to develop solutions that operate autonomously and are capable of collecting data, processing it, and making decisions regarding the behaviour of devices. One such solution is multi-agent systems.

Multi-agent systems (MASs) are particularly well suited for studying Smart Grid system implementation, such as a collection of at least two or more (artificial) agents, where the word agent can be succinctly described as an artificial entity that can act in its environment [1]. It is implicitly assumed that they are computational by design, that is, a decision about an action "can be broken down into primitive operations that can be implemented in a physical device" [7]. There exist several studies taking a MAS approach to studying community-based markets for electricity energy trading.

In the article [5], the authors presented a three-element architecture of the smart grid system, outlining elements such as Perception, Network, Service and Application Layer. In terms of possible applications of multi-agent systems, in addition to the levels presented, multi-agent systems allow for the division of the network layer into communication with IoT devices and communication between agents. The primary role of multi-agent systems is to provide control functions and assist communication in smart grid systems, particularly in microgrid systems [8]. Such a division of communication in smart grid systems relates to the security postulates of the systems, as discussed in the study [6]. Multi-agent systems, by their nature, resemble the concept of P2P systems used in smart grid theory [9], [11], but they have several additional features. These include the ability to define an agent's artificial intelligence mechanisms, dedicated communication standards that ensure the design patterns of the communication being conducted, agent mobility, and negotiation mechanisms. In the case of smart grids, the application of auction systems in the area of energy sharing [12], [13] can be facilitated by agents in the construction of auction systems, supported by agents. In the present article, the multi-agent system is examined within the context of a digital twin, wherein individual agent entities simulate the functioning of the network using real-world data. The simulation was developed based on the proposed algorithm and uses one of the machine learning models

III. Materials and Methods

This article used the literature analysis method. The literature review of the impact of multi-agents on the smart grid is detailed by the assumptions of smart grid security, adaptability, and user-friendliness factors. The data set of publications in the Web of Science was examined. The first query in the topic "Smart grid and security" referred to 5.888 publications discovered between 1900 and 2023. The topic was studied mostly by topics connected with the power grid, renewable energy resources, and the Internet of Things.

The previous studies and the state-of-the-art of smart grids concerning the surveys in different contexts. The most cited research about the security of smart grid by Fang et al. [3] showed the smart grid survey till 2011 as a new and improved power grid and showed the security features in IoT applications of smart grid, smart transportation, and smart cities, to demonstrate how fog/edge computing based IoT should be implemented in real world. Ellabban, Abu-Rub, and Blaabjerg showed the status, prospects, and enabling technology of renewable energy resources [4]. Lin et al. showed the architecture, enabling technologies, security and privacy, and applications of the Internet of Things [5]. Yan et al highlighted the major motivations, requirements, and challenges in smart grid communication infrastructures [6], as well as Mo et al. showed the vision of a secure smart grid infrastructure [33], and S. Sridhar et al. [34]. Deilami et al. presented the new real-time smart load management (RT-SLM) control strategy for coordinating the charging of multiple plug-in electric vehicles (PEVs) in a smart grid system performed by a utility energy distribution system [32]. The examples of the most cited studies were connected with smart-grid security issues, i.e., security technology for smart-grid networks, malicious data attacks on the smart grid with intrusion detection techniques for cyber-physical systems, and classifications and applications of physical layer security techniques for confidentiality.

A. The Literature Review Method

The research methodology was based on the literature review and research questions RQ1 and RQ2. The research questions were based on the research gap present in the previous research studies. The following query was formulated to verify the previous findings described as RQ1: Security aspects query: "Multi-Agents" AND "Smart Grid" AND "Security". Data collected from the Web of Science databases were used. The research findings were evaluated and discussed.

B. Research Results

The research results of RQ1 presented multidisciplinary publications in the field of security multi-agent systems for improving smart grid implementation. There are some features of multi-agent software usage and its role in smart grid systems that have been studied. Based on a review of the literature, the features are presented as research results based on literature review. Multi-agent software affects the security of smart grids, especially in relation to their expansion and modification. It cooperates with other solutions, which is necessary in the context of an intelligent network that is a system of systems with critical infrastructure. As the security solutions used in traditional IT networks are not sufficient for the system of systems [41], in the case of smart grids, such features of multi-agent systems as decentralized decision-making, adaptability, substitutability, communication, learning, mechanisms of trust, cooperation, resilience, and self-healing

gain in importance. As a result, multi-agent systems provide an adequate basis for the construction of security that is required in system of systems and critical infrastructure. Answering the RQ2 the example of studies influence of multi-agents software usage on a smart grid system was presented in Table I.

TABLE I.
INFLUENCE OF MULTI-AGENT SOFTWARE USAGE ON A SMART GRID SYSTEM

Smart Grid Feature	Multi-Agent Influence	Source
Adaptive robotics	Modular systems enable flexible adaptation in production. Human–robot interactions via mobile devices.	[15], [17]
Additive manufacturing	Possibility to individualize products in cost-effective, small batches.	[24]
Automated Home Energy Management	Secure Automated Home Energy Management in Multi-Agent Smart Grid Architecture	[19]
Cybersecurity	Methodologies allowing for automatic detection and response to cyberattacks; adaptive computational intelligent systems continuously evolving; a distributed multi-agent scheme to enhance the cybersecurity of smart power grids.	[28]
Decentralized Intrusion Prevention	Decentralized Intrusion Prevention (DIP) Against Coordinated Cyberattacks on Distribution Automation Systems	[30]
Demand forecasting	The MAS (Multi-Agent System) Model allows the VPP (Virtual Power Plant) to know in advance the amount of power and is based on artificial neural networks (ANNs)	[20]
Energy management	Smart grid management in prosumer communities, trading of energy	[13], [14], [16]
Demand response	Consumers can reduce their energy consumption through load curtailment, shift their energy consumption over time, or generate and store energy at certain times to provide the grid with more flexibility.	[21], [23]
User-Friendliness Environment	An effective modeling and simulation environment, in terms of generality, user-friendliness, modeling flexibility, interoperability with GIS datasets, and computational efficiency	[22]

The AI-Knowledge Management Process of implementing the agents in a smart environment could be discovered in future research. Nowadays, the RQ2 answer is based on the description of the AI-Knowledge Management model for agent tools implementation . The background is based on the revised SECI model, with the machine (AI agent) in the knowledge management process that can play an active or a passive role. The active role would generate an output or a response, while the passive role could be compared to listening and adapting/rebuilding the internal (knowledge) representation. Consequently, the four areas would each be split into a human perspective and a machine perspective, leading to eight fields of action in the new GRAI model [25]. More recent versions of LLM-based systems, such as OpenAI ChatGPT or Google Gemini, allow the human user to add additional relevant materials into the conversation, e.g., using the "memory function" of those systems. This context relates to the interaction field as it helps the machine to identify a more precise context with a domain-specific focus in the dialogue. This way, a general conversation can be leveraged toward a specific direction by the human user by providing externalized information to the machine. Another application use case that is emerging rather frequently here is the use of GenAI in retrieval-oriented task using Retrieval Augmented Generation (RAG), which combines an initial search query with specific document collections (externalized information) to derive a more specific search results when the original query is augmented by the generated content from the externalized information [26]. In contrast to the use case of information retrieval in enterprise-specific information sources (enterprise search), in the field of KM, the use of GenAI could introduce a bias in the results that originates from the foundation models used. However, these effects might be similar to the contextual integration of a human user and could be counteracted by carefully selecting and adopting the right foundation model [27]. In the case of a smart grid security project, the design of architecture, algorithms and simulation studies are becoming more important.

The example described in the paper illustrates RQ1 and RQ2 answers.

IV. PRACTICAL EXEMPLIFICATION

As detailed earlier, IoI and IoT underpin Smart Grid oversight and can be leveraged to strengthen the operation of these networks. Multi-agents could support Smart Grid Security, the robotisation of processes, and system adaptiveness. Authors' prior research into Smart Grid security devised a multi-agent system architecture to reinforce its security [18]. The resulting algorithm was calibrated to gauge the Grid's performance in terms of energy drawn by connected devices. In the example shown below, an algorithm for collecting information from IoT devices is described, the process in which it was used is presented, and a machine learning algorithm is employed to evaluate the collected data. The proposed algorithm was validated via a simulation conducted under the Digital Twin paradigm on the Jade platform. One possible application of IoT and Smart grid solutions is to support the monitoring of user and property security. The subsequent analysis concerns the Home Area Network (HAN) and Neighbourhood Area Network (NAN), where devices are examined locally, either within a single building or across multiple buildings in a given area. Home security systems, such as burglar alarms, sensors, can be supported by IoT devices and generate events related to the breach of defined rules. A problem encountered in IoT systems is the low performance of devices designed for minimal power consumption. In such solutions, it is crucial to use ML algorithms with low resource demands. For this experiment, we used the Isolation Forest algorithm. It is recognised for its low resource requirements.

The literature review [36], [37] allowed for an attempt at specifying an algorithm to support the operation of the network within the framework of IoI and IoT theory using a digital twin theory. To illustrate the conducted research experiment, elements of the architecture of a prototype using business process modelling and IoTDT-BPMN notation were developed. Fig. 2 presents the process of the system's operation

based on IoTDT-BPMN elements. Each pool constitutes a set of tasks executed by the individual devices used when experimenting.

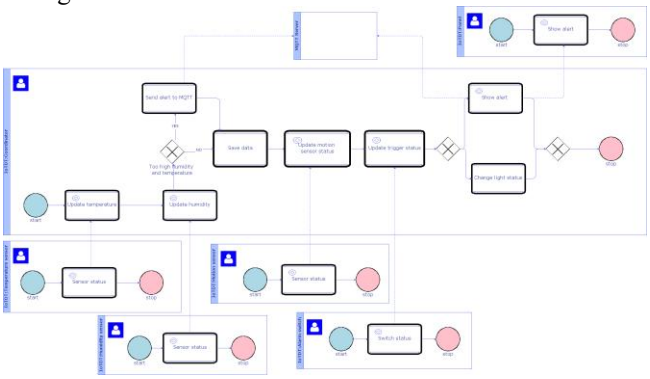

Fig 2. A process in the extended BPMN notation depicting the operation of the simulated system

The whole experiment was developed based on a JADE multi-agent system, which was used to perform the simulation. All the devices were registered in a multi-agent system, and agents' specific behaviours were defined. The implementation uses the IotDTBPMN2Jade algorithm available at GitHub [40]. Activation of the simulation led to the generation of communication between the agents, which resulted in the sending of a notification about a detected event and the development of a knowledge base of alert events. Data from the available sensors was gathered using the developed solution after the simulation phase. The data shown in the figure were collected from an IoT sensor connected to an MQTT server between 26 May 2025 and 8 May 2025. Two pronounced "spikes" in humidity levels can be observed, corresponding to emergency shutdowns of the ventilation system on 2 May 2025 and 4 May 2025. After this initial stage, the sensor readings were used to develop a model based on the Isolation Forest algorithm. One requirement of the algorithm is that the input data must be supplied at regular time intervals. In this project, the raw sensor readings were resampled into five-minute intervals. Since the sensor conserves power by reporting only when its state changes, any missing values were filled using linear interpolation. This ensured that every time slot was represented in the training set. The conducted experiments showed that, with the number of trees set to n_estimators=200 and a contamination level of 0.2 %, the model produced anomaly predictions that closely matched the real-world events illustrated in Fig. 3.

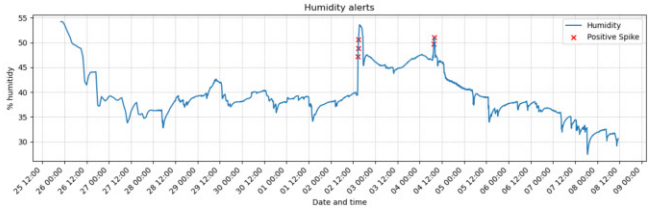

Fig 3. Outcomes of using the ML algorithm (humidity alerts)

The model flagged 5 points as anomalies from the initial 3,617 samples, which is about 0.14%. Increasing the contamination level to 0.5% raised the number of alerts to 12, while lowering it to 0.05% caused it to miss all anomalies. In the subsequent model test, a three-day dataset was prepared containing two events characterised by sudden spikes in humidity levels. The model's results on this simulated data are shown in Fig. 4. The model correctly detected the humidity spikes, indicating that the recommended 50% threshold was exceeded.

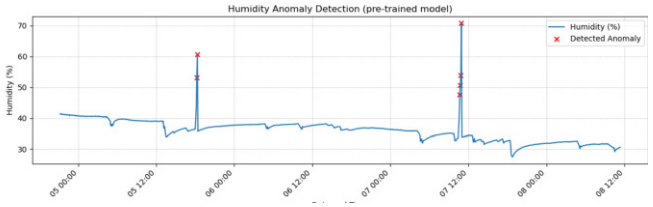

Fig. 4. Humidity anomaly detection

V. Conclusion

The paper showed the studies of theoretical and practical exemplification of multi-agents software security due to RQ1 and RQ2. The proposed research methodology was based on literature and focused on an IoT alarm-monitoring algorithm for smart homes and smart grids, which was described using an expanded BPMN notation and built on the idea of a digital twin. The algorithm specifies how agents evaluate the need to trigger alarms for particular model parameters and may serve to simulate the behaviour of IoT devices within Smart Grid networks. The algorithm's mechanism for gathering parameters from IoT devices offers further extension through the use of a SIEM-Connector concept. This idea involves a service provider continuously monitoring a large number of devices across several networks. Such integration allows real-time detection of threats reported by multiple domestic networks simultaneously. The use of the Isolation Forest algorithm facilitated the model's training and its effective identification of situations that could threaten the system's operational continuity. This was verified by the conducted simulation. The future research should be concerned with the implementation and usage of the AI-based Knowledge Management (AI-KM) models with GenAI and the internalization interaction between the machine agents. Internalization relates strongly to the creation of internal models (or representations) of the knowledge of the outer world of the agent, reflecting the views and beliefs of the agent. The assistance by GenAI might both help the internalization processes of the human agent, but might also be beneficial to proactively build or adapt (digital) representations for the machine agent.

References

[1] Q. Tang, F. R. Yu, R. Xie, A. Boukerche, T. Huang and Y. Liu, "Internet of Intelligence: A Survey on the Enabling Technologies, Applications, and Challenges" in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1394-1434, third quarter 2022, doi: 10.1109/COMST.2022.3175453

[2] A. Okino Otuoze, A. Masood, R. Larik "Smart grids security challenges: Classification by sources of threats". Journal of Electrical Systems and Information Technology 5(2018) 468-482, https://doi.org/10.1016/j.jesit.2018.01.001

[3] X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in *IEEE Communications* Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012, doi: 10.1109/SURV.2011.101911.00087

[4] O. Ellabban, H. Abu-Rub, F. Blaabjerg "Renewable energy resources: Current status, future prospects and their enabling technology", Renewable and Sustainable Energy Reviews, vol.39, 748-764, 2014, 10.1016/j.rser.2014.07.113.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200

[6] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 5-20, First Quarter 2013, doi: 10.1109/SURV.2012.021312.00034

[7] D. L. Poole, A. K. Mackworth "Artificial intelligence: foundations of computational agents", Second ed., USA, Cambridge University Press; 2017.

[8] M. L Tuballa, M. L Abundo "A review of the development of Smart Grid technologies", Renewable and Sustainable Energy Reviews, Volume 59, 2016, pp. 710-725, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2016.01.011.

[9] J. Kim and Y. Dvorkin, "A P2P-Dominant Distribution System Architecture," in IEEE Transactions on Power Systems, vol. 35, no. 4, pp. 2716-2725, July 2020, doi: 10.1109/TPWRS.2019.2961330.

[10] F. Moret and P. Pinson, "Energy Collectives: A Community and Fairness Based Approach to Future Electricity Markets," in IEEE Transactions on Power Systems, vol. 34, no. 5, pp. 3994-4004, Sept. 2019, doi: 10.1109/TPWRS.2018.2808961.

[11] T. Morstyn and M. D. McCulloch, "Multiclass Energy Management for Peer-to-Peer Energy Trading Driven by Prosumer Preferences," in IEEE Transactions on Power Systems, vol. 34, no. 5, pp. 4005-4014, Sept. 2019, doi: 10.1109/TPWRS.2018.2834472.

[12] P. Olivella-Rosell, G. Viñals-Canal, A. Sumper, R. Villafafila-Robles, B. A. Bremdal, I. Ilieva, S. Ø. Ottesen "Day-ahead micro-market design for distributed energy resources" In: 2016 IEEE International Energy Conference. 2016, p. 1–6. http://dx.doi.org/10.1109/ENERGYCON.2016.7513961.

[13] W. Tushar, B. Chai, C. Yuen, S. Huang, D. B. Smith, H. V. Poor, Z. Yang "Energy Storage Sharing in Smart Grid: A Modified Auction-Based Approach," in IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1462-1475, May 2016, doi: 10.1109/TSG.2015.251226.

[14] R. Verschae, T. Kato, T. Matsuyama "Energy management in prosumer communities: A coordinated approach", Energies 2016;9(7). http://dx.doi.org/10.3390/en9070562, URL https://www.mdpi.com/1996-1073/9/7/562.

[15] A. Billard, S. Mirrazavi, N. Figueroa "Learning for Adaptive and Reactive Robot Control. A Dynamical Systems Approach", MIT Press, 2022.

[16] R. Jing, MN. Xie, FX. Wang, LX Chen. "Fair P2P energy trading between residential and commercial multi-energy systems enabling integrated demand-side management", Appl Energy 2020;262:114551.

[17] S. Nolfi "Behavioral and cognitive robotics: An adaptive perspective". Roma, Italy: Institute of Cognitive Sciences and Technologies, National Research Council CNR-ISTC (2021).

[18] T. Kisielewicz, S. Stanek S., M. Żytniewski "A Multi-Agent Adaptive Architecture for Smart-Grid-Intrusion Detection and Prevention", Energis, 2022 15, 4726. https://doi.org/10.3390/en15134726.

[19] C. P. Nguyen, A. J. Flueck "Agent based restoration with distributed energy storage support in smart grids", IEEE Trans. Smart Grid, vol. 3, no. 2, pp. 1029–1038, Jun. (2012).

[20] P. Vytelingum, T. D. Voice, S. D. Ramchurn, A. Rogers, N. R. Jennings "Agent-based micro-storage management for the smart grid" in Proc. 9th Int. Conf. Auto. Agents Multiagent Syst., 2010, pp. 39–46.

[21] G. H. Merabet et al., Applications of multi-agent systems in smart grids: A survey, in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), pp. 1088–1094, (2024)

[22] L. Hernández-Callejo et al. A Multi-Agent-System Architecture for Smart Grid Management and Forecasting of Energy Demand in Virtual Power Plants, January 2013, IEEE Communications Magazine 51(1), DOI: 10.1109/MCOM.2013.6400446.

[23] J. R. Vázquez-Canteli, Z. Nagy "Reinforcement learning for demand response: A review of algorithms and modeling techniques", Applied Energy, Volume 235, 2019, pp. 1072-1089, ISSN 0306-2619, https://doi.org/10.1016/j.apenergy.2018.11.002.

[24] I. Blecic, A. Cecchini, G.A. Trunfio "A Software Infrastructure for Multi-agent Geosimulation Applications" In: Gervasi, O., Murgante, B., Laganà, A., Taniar, D., Mun, Y., Gavrilova, M.L. (eds) Computational Science and Its Applications – ICCSA 2008. ICCSA 2008. Lecture Notes in Computer Science, vol 5072, 2008, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-69839-5_28.

[25] K. Böhm, S. Durst "Knowledge management in the age of generative artificial intelligence – from SECI to GRAI", VINE Journal of Information and Knowledge Management Systems Emerald Publishing Limited 2059-5891, 2025, DOI 10.1108/VJIKMS-10-2024-0357.

[26] H. Yu, A. Gan, K. Zhang, S. Tong, Q. Liu, and Z. Liu "Evaluation of retrieval-augmented generation: a survey", arXiv, 2024, doi: 10.48550/arXiv.2405.07437.

[27] P. Zhao, H. Zhang, Q. Yu, Z. Wang, Y. Geng, F. Fu, L. Yang, W. Zhang, J. Jiang, and B. Cui "Retrieval-augmented generation for AI-generated content: a survey", arXiv, 2024,. doi: 10.48550/arXiv.2402.19473.

[28] W. Ben, H. Ines "Preventive mental health care: A complex systems framework environments", Cognitive Systems Research, 84, 101199, 2024, http://doi.org/ 10.1016/j.cogsys.2023.101199

[29] Y. Mo, T. H. -J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli "Cyber–Physical Security of a Smart Grid Infrastructure", in Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.

[30] N. Z. Aitzhan, D. Svetinovic "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams" in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2616861.

[31] J. Appiah-Kubi, C. C. Liu "Decentralized Intrusion Prevention (DIP) Against Co-Ordinated Cyberattacks on Distribution Automation Systems", in IEEE Open Access Journal of Power and Energy, vol. 7, pp. 389-402, 2020, doi: 10.1109/OAJPE.2020.3029805.

[32] S. Deilami, A. S. Masoum, P. S. Moses and M. A. S. Masoum, Real-Time Coordination of Plug-In Electric Vehicle Charging in Smart Grids to Minimize Power Losses and Improve Voltage Profile, in IEEE Transactions on Smart Grid, vol. 2, no. 3, pp. 456-467, Sept. 2011, doi: 10.1109/TSG.2011.2159816.

[33] Y. Mo, T. H. -J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli "Cyber–Physical Security of a Smart Grid Infrastructure", in Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.

[34] S. Sridhar, A. Hahn, M. Govindarasu "Cyber–Physical System Security for the Electric Power Grid". in Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012, doi: 10.1109/JPROC.2011.2165269.

[35] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, X. Yang "A Survey on the Edge Computing for the Internet of Things," in IEEE Access, vol. 6, pp. 6900-6919, 2018, doi: 10.1109/ACCESS.2017.2778504.

[36] B. Karaduman, B. T. Tezel, G. Kardas, M. Challenger "DSML4JaCaMo: A Modelling tool for Multi-agent Programming with JaCaMo", Proceedings of the 19th Conference on Computer Science and Intelligence Systems (FedCSIS), M. Bolanowski, M. Ganzha, L. Maciaszek, M. Paprzycki, D. Ślęzak (eds). ACSIS, Vol. 39, pages 637–642 (2024)

[37] V. Carchiolo, G. Catalano, M. Malgeri, C. Pellegrino, G. Platania, N. Trapani "BPM Tools for Asset Management in Renewable Energy Power Plants", Proceedings of the 2019 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 18, pages 645–649 (2019)

[38] ISO/IEC DIS 27019, https://www.iso.org/standard/85056.html

[39] ISO/IEC 30101:2014, https://www.iso.org/standard/53221.html

[40] GitHub, https://github.com/Anakainosis/IotDTBPMN2Jade

[41] F. Aloul, A.R. Al-Ali, R. Al-Dalky, M. Al-Mardini, El-Hajj, W. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy. 1. 1-6. 10.12720/sgce.1.1.1-6. (2012).