An end-to-end approach for scalable real time Anomaly detection in smart buildings

Evangelos Karakolis
Decision Support Systems Laboratory
School of Electrical & Computer Engineering
National Technical University of Athens
Athens, Greece
vkarakolis@epu.ntua.gr

Konstantinos Alexakis
Decision Support Systems Laboratory
School of Electrical & Computer Engineering
National Technical University of Athens
Athens, Greece
kalexakis@epu.ntua.gr

Panagiotis Kapsalis
Decision Support Systems Laboratory
School of Electrical & Computer Engineering
National Technical University of Athens
Athens, Greece
pkapsalis@epu.ntua.gr

Spiros Mouzakitis
Decision Support Systems Laboratory
School of Electrical & Computer Engineering
National Technical University of Athens
Athens, Greece
smouzakitis@epu.ntua.gr

John Psarras
Decision Support Systems Laboratory
School of Electrical & Computer Engineering
National Technical University of Athens
Athens, Greece
john@epu.ntua.gr

***Abstract*— Internet of things (IoT) along with big data technologies can accrue significant added value in several domains and improve people's everyday life. One of the domains that can be benefitted the most by the aforementioned technologies is Smart Buildings. This is because, several aspects of people's everyday lives can be improved through IoT services, such as energy consumption, health, heating, building security and more. IoT services can be divided to near real-time, and static based on the time that they require in order to return results. Significant amount of research papers has been dedicated to the second for services such as energy forecasting, while for near real-time services there are not so many publications, while, most of the existing ones focusing mostly on obtaining meaningful results. In this publication we propose a conceptual architecture for building a near real-time Anomaly Detection service for smart buildings using the Fog Computing paradigm, to achieve scalability and low latency. Moreover, we provide a technical glance of the proposed solution, suggesting specific technologies for each functionality as well as restrictions for each technology. It is worth mentioning that the proposed approach can be easily adapted for other near real-time services with little modifications.**

Keywords— Smart Buildings; Anomaly detection; IoT; Fog Computing; Edge Computing; Stream Processing; Bloom Filter; Cloud Computing

I. INTRODUCTION

In the last decade, Internet of Things (IoT) has been among the most popular trends, towards the digital transformation of business and technology. This is because, it can unlock significant added value for both customers and companies [1, 2] and improve the quality of people's lives by bringing closer the digital and the physical world. Specifically, according to McKinsey in 2021 [3], the potential economic value that the IoT could unlock is large and growing and it is estimated that, by 2030, it could enable $5.5 trillion to $12.6 trillion in value globally, including the value captured by consumers and customers of IoT products and services. Several different sectors can be benefitted by IoT technologies, including (but not limited to) health, factories, cities, vehicles, and buildings.

Of course, the tremendous success of the IoT in the last few years, goes hand in hand with the rapid advancements of Big Data Analytics and Cloud Computing technologies. In particular, Big Data Analytics enable the processing of large-scale volumes of data in a very efficient manner, while traditional database technologies fail to provide acceptable response times with such large volumes of data. Of course, big data do not imply only large volumes of data, instead the term implies also high velocity (speed at which new data is generated and move around), variety (meaning that data is not always structured and cannot be stored directly to relational databases), veracity (meaning that data with wrongful values are also included), and value meaning that businesses that invest to big data technologies should require a return on investment (5 Vs of Big Data [4]).

On the other hand, cloud computing provides a set of network enabled services, providing scalable, Quality of Service (QoS) guaranteed, normally personalized computing infrastructures on demand, which could be accessed in a simple and pervasive way [5]. Moreover, it provides Software as a Service (SaaS) and Platform as a Service (PaaS) capabilities, that make the IoT data handling easier and more reliable than ever before.

With the rise of IoT and Big Data Analytics, significant value adding services can be unlocked for smart buildings. On the one hand, this needs to be done as buildings are responsible for a significant amount of energy consumption (40% of EU energy consumption), and therefore the building sector can play a key role on effective climate policy [6,7] and on the other hand residents can be benefited in several aspects of their everyday life such as health and security [8].

In this context, several services and applications have already been developed in order to improve residents' health, energy consumption and security of smart buildings, based on both real time and static data. Some examples are clustering of electricity consumption [9], occupancy detection (e.g. [10]), electrical load forecasting [11] and anomaly or outlier detection [12]. However, most of the work that has been conducted focuses mostly on processing static data and drawing inferences from them. At the same time, the literature for services that respond in real time focuses mostly on the results and follows a centralized cloud approach that is not scalable for a grid of smart buildings.

In this paper, we deal with the problem of real time anomaly detection in smart buildings. Unlike other works, we focus mostly on the technological aspect of the solution, taking into consideration scalability and response times as the utmost priorities of this work. As a result, we propose a conceptual architecture that is based on the Fog Computing paradigm [13] and provides a scalable approach for solving the problem of anomaly detection in real time. With this paradigm, the computation is distributed across three different layers, the Edge, the Fog and the Cloud. Hence, the computation takes place closer to the edge devices instead of being performed entirely in the cloud. This results to faster computation and hence faster response times and alerts. Moreover, we propose several suitable technologies, along with explanations of their functionalities and their specific role to the proposed solution.

This work has been conducted under the context of the EU funded research project I-NERGY [14] that aims at evolving, scaling up and demonstrating innovative AI-as-a-Service (AIaaS) Energy Analytics Applications and digital twins services that will be validated along 9 pilots, which a) span over the full energy value chain, ranging from optimized management of grid and non-grid Renewable Energy Sources (RES) assets, improved efficiency and reliability of electricity networks operation, optimal risk assessment for energy efficiency investments planning, optimizing local and virtual energy communities involvement in flexibility and green energy marketplaces; and b) delivers other energy and non-energy services to realize synergies among energy commodities (district heating, buildings) and with nonenergy sectors (i.e., e-mobility, personal safety/security, AAL), and with non- or low-technical domains end users (i.e., elderly people).

The rest of the paper is organized as follows: In Section II, we provide a brief overview of works that relate to this publication, along with a brief overview of the basic concepts and technologies that are proposed. Section III presents the proposed conceptual architecture for anomaly detection in smart buildings, based on the Fog Computing paradigm. Furthermore, several technologies that are proposed to be used are discussed. Section IV discusses the advantages of the proposed approach, as well as several aspects that are not covered by the proposed solution. Last but not least, section V concludes the paper and provides several issues that will be addressed in future extensions of this work.

II. Related Work

The work that has been conducted in the context of this publication has its roots on several scientific fields. Specifically, it combines IoT technologies, with big data and stream processing along with the fog computing paradigm, in order to facilitate scalable and near real time anomaly detection, for smart buildings. There are plenty of scientific publications in these fields, however, at the time of writing this article, an approach that serves as an end-to-end scalable solution for anomaly detection in citizen behavior in smart buildings was missing from the literature. In this section, several related publications are presented in a nutshell.

The proposed architecture is based on the Fog Computing paradigm, which is an implementation of Edge Computing [15], as it provides distributed computing, storage, control and networking capabilities closer to the user (edge). However, it is not yet another implementation of Edge Computing but rather the highest evolution of Edge Computing principles, providing a structured intermediate layer that fully bridges the gap between IoT and Cloud computing [16].

There are several publications that use the Fog Computing paradigm. For instance, [17] proposes an algorithm for efficient utilization of resources in the network infrastructure. The approach is generic and the results can be used as a micro-benchmark in studies related to Edge and Fog Computing applications. Abbasi et al. [18], studied the resources management and allocation as well. They developed two methods to balance the power consumption at the edge of the network and reduce delays in the processing of workflows, resulting to minimized communication delay between the cloud and fog nodes. Moreover, Mohamed et al. [19] studied the utilization of a Service-Oriented Middleware (SOM) for Cyber-Physical Systems (CPS), which is compatible with systems based on Cloud and Fog Computing.

Apart from optimal resource allocation applications, several services based on the Fog Computing paradigm have been developed. First of all, Cheng et al. [20], developed a programming model named FogFlow for IoT smart city platforms, utilizing the fog computing paradigm to overcome the scalability issues that arise in smart city infrastructures. FogFlow focuses on interoperability and openness, to enable IoT service developers to program elastic IoT services easily over cloud and edges. Moreover, it supports standard interfaces to share and reuse contextual data across services. Finally, a use case for anomaly detection of energy consumption in smart cities is presented.

In addition, Wang et al. [21], presented an IoT service architecture that is based on cloud and edge computing and focuses on security. Their experiments showcased that this edge-based architecture can improve both the security and efficiency of IoT-Cloud systems.

Regarding Smart buildings and smart grids, among the most popular services in the literature are the ones for Energy Forecasting. For instance, [11] provides an overview of the proposed load forecasting approaches in smart buildings, presenting the results of several methods. Furthermore, several models for energy consumption prediction are examined at [22], and several Machine Learning models were deployed and tested in a real-world Smart Building testbed, with modest results due to the small size of the dataset that was used. Of course, there exists a much larger number of studies related to energy forecasting than the ones that were already presented [23-27].

However, Energy forecasting services in most cases are not real time and therefore services for Occupancy Detection and Anomaly Detection and Identification are closer to the subject of this publication, as they require near real-time response at a very low latency. Both the aforementioned types of services have been examined in the literature. For instance, regarding Occupancy Detection, Oldewurtel et al. [28] examined the potential of using occupancy information to realize a more energy efficient building climate control. They developed a Model Predictive Control framework, in order to evaluate the energy savings potential, in comparison to other strategies. Elkhoukhi et al. [10] combined occupants' information, with sensor data to achieve better results and real-time responses. Other publications that focus on Occupancy detection are [29,30].

Concerning anomaly detection and identification, most of the studies focus either on people's daily life and health or on security. Regarding people's daily life, Yahaya et al. [31] introduced a new approach of creating an ensemble of novelty detection algorithms based on the concept of internal and external consensus. The results of the study showed that the proposed approach can successfully identify anomalous instances. Novak et al. [32], identified and addressed several weaknesses of the existing approaches (inactivity, detection only on a daily basis). This approach was based on semi-supervised clustering models of Self Organized Maps (SOMs) and the results were evaluated in both synthetic and real data for a two-month period. Other publications regarding anomaly detection in people's behavior are [33-37].

Concerning Anomaly detection focused on security, Dahmen et al. [38] introduced an activity-aware approach to security monitoring and threat detection in smart buildings. The proposed method was evaluated against the CASAS smart home dataset [39]. Other publications for anomaly detection that focus on security are [40, 41].

Other IoT applications and services for smart buildings and smart grids that have been reported in the literature, are focusing on predictive maintenance [42], demand response [43], indoor location identification [44], fire and smoke detection [45], intrusion detection [46]. However, they will not be presented further in the context of this publication.

It is worth mentioning that there are several existing specifications for data-driven initiatives and underlying B2B reference architectures at the interplay among smart buildings, AI, IoT, Big Data, smart energy grids, industry / manufacturing, including IFC [47], OGC CityGML [48], BDVA SRIA4.0 [49], COSMAG [50], FIWARE Smart Energy Reference Architecture [51], IDSA data sovereignty conceptual architecture [52] and IoT/edge AIOTI [53] High Level Architecture, towards a living Reference Architecture specifically tailored to the buildings value chain. Moreover, indicative architectures and frameworks for AI and data democratization for intelligent energy management are presented at [54-57]. However, all the aforementioned initiatives are too generic including many components that are not useful for the specific use case. Of course, with future extensions of our work the alignment with already existing standards and specifications will be examined thoroughly.

III. Proposed Approach for Anomaly Detection in Citizen Patterns in Smart Buildings

In this section a conceptual architecture based on the Fog Computing paradigm is proposed, in order to address the problem of anomaly detection in citizen patterns in smart buildings efficiently in terms of both scalability and low latency. This is achieved by distributing the computation to edge and fog nodes instead of the cloud and leads to faster results and lower network traffic as well as lower cloud workload. The proposed architecture is accompanied by several underlying technologies that can contribute to a more efficient solution.

In Figure 1, the proposed conceptual architecture is illustrated. In particular, it consists of three layers, the Edge layer, the Fog layer and the Cloud layer. The Cloud layer is the centralized high-performance infrastructure, where centralized computationally intensive processes take place. It is connected with several fog instances of the fog layer, which are responsible for less computationally intensive tasks. Finally, each Fog instance, is connected to one or more edge instances, that have little to no computational resources.

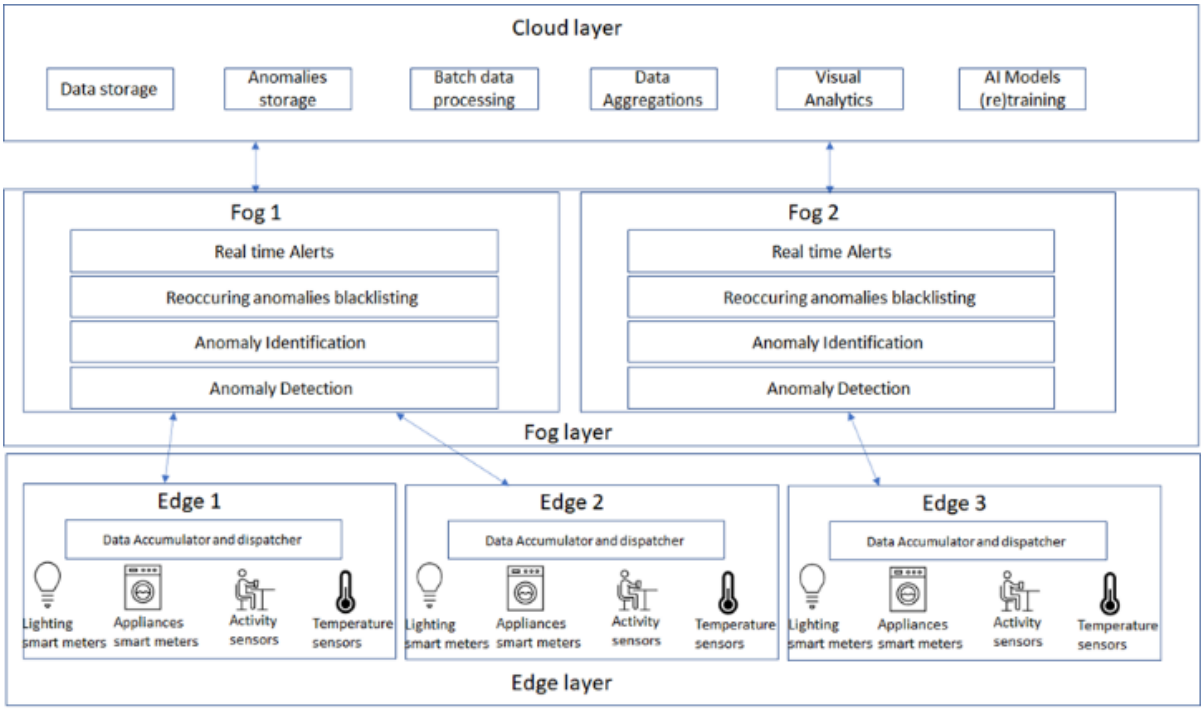

Fig. 1. Conceptual Architecture for Anomaly detection in smart buildings

A. Edge Layer

The edge layer consists of several sensors and actuators including lighting, appliances and energy smart meters as well as sensors for activity tracking, temperature etc. that are monitored by a gateway device (Data Accumulator and

Dispatcher) that notices any changes on the state of the former and sends a message to a message queuing engine, in order to let the related fog and cloud applications know about the changes. Moreover, it can receive messages for configuration by its related fog in order to update the edge devices accordingly.

B. Fog Layer

The fog layer has more computational resources than the edge layer but significantly less than the cloud one. Therefore, this layer can be used for tasks that are not computationally and memory intensive. It has a small workload, only receiving messages for specific edge instances and limited power for computations. Such tasks include data filtering, counting distinct elements and other simple operations. In addition, it is close to the edge and can provide immediate responses for simple operations.

In this context, it is capable of executing rule-based anomaly detection operations, for instance identify as outliers data points that deviate significantly from the majority of data points. Of course, anomalies can be identified also through ML/AI models, however a complex model that needs significant amount of memory to be stored or run is not appropriate for the fog layer. On the other hand, simple models can be stored and run in the fog easily.

Another operation that can be executed in the fog layer is Anomaly identification. This can be done after recognizing an anomaly data point. As a next step, at fog level, it is feasible to calculate the distance between the identified anomaly and the centroid of each type of anomaly and select the nearest neighboring centroid as the type of anomaly for the specific data point.

Apart from filtering and anomaly type identification, it is useful and feasible to apply some kind of blacklisting for reoccurring anomalies. This can be done by storing the type of anomaly along with the instance id that caused the anomaly. However, in case there is a big number of anomalies and limited memory, this can be done also through bloom filters [58]. A bloom filter is a mechanism that enables to quickly test if an item is part of a set, without storing the set items. It guarantees that if an item was not found in the set by the bloom filter then it is not a member of the set, while if an item is found in the set it will be a member of the set with high probability. In the case of anomaly detection if the bloom filter decides that a data instance is not in the list of anomalies then it certainly is not. While, in case the bloom filter decides that the instance is in the list of anomalies then it is with high probability. Of course, the list of anomalies should be reinitialized periodically (e.g. once a day) as an anomaly should not be considered as reoccurring if a long time period has passed.

On top of the Anomaly detection, Anomaly Identification and reoccurring anomalies blacklisting services an alerts service can also be part of the fog layer. This alerting service is responsible for sending alerts to the subscribed user once an anomaly is identified, along with its type. Moreover, if the anomaly is reoccurring, it can send alerts to more interested parties, or increase the severity of the alert.

C. Cloud Layer

The cloud layer is the centralized computation layer that has tremendous computational power and memory compared to the other layers. Also, it is accompanied by heavy network traffic as it receives data and requests from several fog instances as well as from numerous edges. Therefore, it cannot guarantee quick responses for the services that provides. Instead, it is suitable for tasks that are computationally or memory intensive, such as batch processing or storing the data. Thus, the proposed conceptual architecture includes services like sensor and anomalies data storage, batch data processing, analytics and data aggregations, exploration and visual analytics in data, as well as AI models training and evaluation. Of course, in a grid of smart buildings more services than anomaly detection are expected to be deployed both in the cloud and the fog, which means that the conceptual architecture would be much more complex if all the potential smart building services were added.

D. Technical Implementation

From a technical point of view, each layer should follow a different approach for its services. Specifically, the edge layer includes the sensors and actuators of the smart building as well as an IoT gateway device. IoT gateways bridge devices and sensors of a smart building to the internet. In order to select an IoT gateway device, the user should make sure that it is compatible with the devices that are intended to be connected as well as the supported communication protocols [59]. Most cloud service providers have their own IoT gateway devices.

Regarding the communication protocols for the edge layer, it is of utmost important to select a proper one in order for the system to work effectively. The most usual choices for IoT applications are the protocols AMQP and MQTT. However, the selection of a protocol should be decided according to the application needs as concluded also at [60].

Concerning the fog layer, all services should be lightweight. In addition, they should consume the messages sent by the edge layer, reading the updates in data and providing the results to a message broker, in order to be received by the cloud layer. They can read the IoT data directly from the IoT gateway device, however another technology that enables messaging through the publish subscribe messaging pattern can be used as well. In specific, Apache Kafka [61] is among the most suitable technologies for publish subscribe messaging for an end-to-end solution such as an entire IoT system using the Fog Computing paradigm. This is because it enables performant data pipelines, storage of massive amounts of messages and integration of different business applications in real time. Moreover, Kafka distributes the messages in topics (channels). This is very important because services can access data only from topics in which they are subscribed.

Last but not least, the cloud layer is responsible for storing and processing the data received from the other layers. Different (mostly noSQL) database technologies can be used for storage such as MongoDB [62]. Regarding the batch and big data processing several technologies can be used such as Apache Spark [63] and Hadoop [64].

IV. Evaluation, Discussion and Limitations

Significant amount of research has been dedicated to IoT services in smart buildings, while most of the research papers are dedicated to static services that depend on historical data. On the other hand, near real-time IoT services can unlock significant added value. Several near real time IoT services are

proposed in the literature. However, in most cases they are focused on the results of the developed service and not paying attention to the response times and the scalability potential of the reported services. Moreover, it is worth mentioning that the cloud computing paradigm which is the most common paradigm on IoT applications, is not suitable for providing near real time services due to the fact that the cloud resources are shared across different buildings and large numbers of edge devices. Hence, even in cases where response times are acceptable, the cloud computing solution is not scalable.

In this context, in the paper at hand we focus on acceptable response times as well as scalability of the proposed service across the entire network. Moreover, instead of the traditional cloud computing paradigm, we present our service under the perspective of the Fog Computing paradigm, defining clearly the processes executed in each layer (Edge, Fog, Cloud). In more detail, we present an end-to-end scalable architecture for real time Anomaly Detection in smart buildings, that utilizes the fog computing paradigm as the most suitable one for large scale IoT applications. Furthermore, the main technologies that can be used in each layer are discussed in brief along with several restrictions that may pose, in terms of resources requirements.

Of course, the presented architecture is accompanied by several limitations. Specifically, security and privacy are not taken into consideration, even though they are extremely important. Several concerns about privacy and security of the proposed architecture have to do with limited network visibility, ineffective ways of attack detection, malicious fog node issues and more [65].

Another important issue that is not discussed in the current publication is interoperability. The problem is that heterogeneous systems and different service providers do not share any common interface in order to understand and consume heterogeneous data safely. Although several interoperability schemes have been proposed (e.g., SAREF [66]), there is no commonly accepted one to be used by all service providers and systems..

V. Conclusion and Future Extensions

This publication provides a scalable end to end approach for near real time anomaly detection in smart buildings using the Fog Computing paradigm, along with the underlying technologies of each computational layer. Up until the moment of writing this publication the literature was missing such an end-to-end approach for real time IoT services in smart buildings.

Moreover, it is worth mentioning that the current approach poses several limitations in terms of security and privacy and interoperability. These pillars will be among the first priorities for future extensions of this study.

Of course, the first priority will be to apply the proposed approach and its underlying technologies and architecture to a real time environment and evaluate the results in terms of quality, latency and scalability. Moreover, the provided services will be evaluated by actual users.

As a next step, privacy issues will be addressed. Specifically, an identity and access control management component that will secure that only authenticated users will have access to services and data will be integrated to the proposed solution. Furthermore, these users will have access only to resources that they are authorized to access. Regarding security concerns, several solutions will be examined such as data encryption and monitoring of virtual machines.

Concerning interoperability, several available interoperability schemes for smart buildings and cities will be examined and extended if needed, according to the project needs in terms of the provided data and the pilot requirements.

Apart from Anomaly detection in citizen patterns in smart buildings, I-NERGY project offers a large gamma of energy analytics services both static and real time for several different EPES stakeholders covering the whole energy value chain. Therefore, new services will be developed, including energy forecasting, flexibility forecasting and demand response, predictive maintenance and more.

Acknowledgment

This work has been funded by the European Union's Horizon 2020 research and innovation programme under the I-NERGY project, Grant Agreement No 101016508.

References

[1] F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," Business and Information Systems Engineering, vol. 57, no. 3. 2015, doi: 10.1007/s12599-015-0383-3.

[2] I. C. L. Ng and S. Y. L. Wakenshaw, "The Internet-of-Things: Review and research directions," Int. J. Res. Mark., vol. 34, no. 1, 2017, doi: 10.1016/j.ijresmar.2016.11.003.

[3] McKinsey, "IoT value set to accelerate through 2030: Where and how to capture it," 2021.

[4] Ishwarappa and J. Anuradha, "A brief introduction on big data 5Vs characteristics and hadoop technology," in Procedia Computer Science, 2015, vol. 48, no. C, doi: 10.1016/j.procs.2015.04.188.

[5] L. Wang et al., "Cloud computing: A perspective study," in New Generation Computing, 2010, vol. 28, no. 2, doi: 10.1007/s00354-008-0081-5.

[6] E. Commission, "Energy use in buildings."

[7] C. C. United Nations, "The Paris Agreement." .

[8] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications," Autom. Constr., vol. 101, 2019, doi: 10.1016/j.autcon.2019.01.023.

[9] Y. Wang, Q. Chen, C. Kang, and Q. Xia, "Clustering of Electricity Consumption Behavior Dynamics Toward Big Data Applications," IEEE Trans. Smart Grid, vol. 7, no. 5, 2016, doi: 10.1109/TSG.2016.2548565.

[10] H. Elkhoukhi, Y. Naitmalek, A. Berouine, M. Bakhouya, D. Elouadghiri, and M. Essaaidi, "Towards a Real-time Occupancy Detection Approach for Smart Buildings," in Procedia Computer Science, 2018, vol. 134, doi: 10.1016/j.procs.2018.07.151.

[11] S. Hadri, Y. Naitmalek, M. Najib, M. Bakhouya, Y. Fakhri, and M. Elaroussi, "A comparative study of predictive approaches for load forecasting in smart buildings," in Procedia Computer Science, 2019, vol. 160, doi: 10.1016/j.procs.2019.09.458.

[12] M. Peña, F. Biscarri, J. I. Guerrero, I. Monedero, and C. León, "Rule-based system to detect energy efficiency anomalies in smart buildings, a data mining approach," Expert Syst. Appl., vol. 56, 2016, doi: 10.1016/j.eswa.2016.03.002.

[13] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. Goren, and C. Mahmoudi, "Fog Computing Conceptual Model," NIST Spec. Publ., vol. 500–325, 2018.

[14] "I-NERGY project," 2021.

[15] E. Karakolis et al., "Artificial Intelligence for Next Generation Energy Services across Europe – The I-NERGY Project," 2022.

[16] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," 2017, doi: 10.1109/GIOTS.2017.8016213.

[17] M. De Donno, K. Tange, and N. Dragoni, "Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog," IEEE Access, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2947652.

[18] M. Taneja and A. Davy, “Resource aware placement of IoT application modules in Fog-Cloud Computing Paradigm,” 2017, doi: 10.23919/INM.2017.7987464.

[19] M. Abbasi, M. Yaghoobikia, M. Rafiee, A. Jolfaei, and M. R. Khosravi, “Efficient resource management and workload allocation in fog–cloud computing paradigm in IoT using learning classifier systems,” Comput. Commun., vol. 153, 2020, doi: 10.1016/j.comcom.2020.02.017.

[20] N. Mohamed, S. Lazarova-Molnar, I. Jawhar, and J. Al-Jaroodi, “Towards Service-Oriented Middleware for Fog and Cloud Integrated Cyber Physical Systems,” 2017, doi: 10.1109/ICDCSW.2017.49.

[21] B. Cheng, G. Solmaz, F. Cirillo, E. Kovacs, K. Terasawa, and A. Kitazawa, “FogFlow: Easy Programming of IoT Services Over Cloud and Edges for Smart Cities,” IEEE Internet Things J., vol. 5, no. 2, 2018, doi: 10.1109/JIOT.2017.2747214.

[22] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, “A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing,” IEEE Internet Things J., vol. 6, no. 3, 2019, doi: 10.1109/JIOT.2018.2870288.

[23] S. Bourhnane, M. R. Abid, R. Lghoul, K. Zine-Dine, N. Elkamoun, and D. Benhaddou, “Machine learning for energy consumption prediction and scheduling in smart buildings,” SN Appl. Sci., vol. 2, no. 2, 2020, doi: 10.1007/s42452-020-2024-9.

[24] T. Ahmad, H. Chen, Y. Guo, and J. Wang, “A comprehensive overview on the data driven and large scale based approaches for forecasting of building energy demand: A review,” Energy and Buildings, vol. 165. 2018, doi: 10.1016/j.enbuild.2018.01.017.

[25] K. Amasyali and N. M. El-Gohary, “A review of data-driven building energy consumption prediction studies,” Renewable and Sustainable Energy Reviews, vol. 81. 2018, doi: 10.1016/j.rser.2017.04.095.

[26] A. González-Vidal, A. P. Ramallo-González, F. Terroso-Sáenz, and A. Skarmeta, “Data driven modeling for energy consumption prediction in smart buildings,” in Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017, 2017, vol. 2018-January, doi: 10.1109/BigData.2017.8258499.

[27] M. A. Alduailij, I. Petri, O. Rana, M. A. Alduailij, and A. S. Aldawood, “Forecasting peak energy demand for smart buildings,” J. Supercomput., vol. 77, no. 6, 2021, doi: 10.1007/s11227-020-03540-3.

[28] I. Sülo, Ş. R. Keskin, G. Doğan, and T. Brown, “Energy Efficient Smart Buildings: LSTM Neural Networks for Time Series Prediction,” 2019, doi: 10.1109/Deep-ML.2019.00012.

[29] F. Oldewurtel, D. Sturzenegger, and M. Morari, “Importance of occupancy information for building climate control,” Appl. Energy, vol. 101, 2013, doi: 10.1016/j.apenergy.2012.06.014.

[30] C. de Bakker, M. Aries, H. Kort, and A. Rosemann, “Occupancy-based lighting control in open-plan office spaces: A state-of-the-art review,” Building and Environment, vol. 112. 2017, doi: 10.1016/j.buildenv.2016.11.042.

[31] T. Labeodan, W. Zeiler, G. Boxem, and Y. Zhao, “Occupancy measurement in commercial office buildings for demand-driven control applications - A survey and detection system evaluation,” Energy and Buildings, vol. 93. 2015, doi: 10.1016/j.enbuild.2015.02.028.

[32] S. W. Yahaya, A. Lotfi, and M. Mahmud, “A Consensus Novelty Detection Ensemble Approach for Anomaly Detection in Activities of Daily Living,” Appl. Soft Comput. J., vol. 83, 2019, doi: 10.1016/j.asoc.2019.105613.

[33] M. Novak, J.F., and L.L., “Anomaly detection in user daily patterns in smart-home environment,” J. Sel. Areas Heal. Informatics, vol. 3, 2013.

[34] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, “Anomaly Detection in Smart Home Operation from User Behaviors and Home Conditions,” IEEE Trans. Consum. Electron., vol. 66, no. 2, 2020, doi: 10.1109/TCE.2020.2981636.

[35] U. A. B. U. A. Bakar, H. Ghayvat, S. F. Hasanm, and S. C. Mukhopadhyay, “Activity and anomaly detection in smart home: A survey,” in Smart Sensors, Measurement and Instrumentation, vol. 16, 2016.

[36] E. Hoque, R. F. Dickerson, S. M. Preum, M. Hanson, A. Barth, and J. A. Stankovic, “Holmes: A comprehensive anomaly detection system for daily in-home activities,” 2015, doi: 10.1109/DCOSS.2015.20.

[37] H. Ghayvat et al., “Smart aging system: Uncovering the hidden wellness parameter for well-being monitoring and anomaly detection,” Sensors (Switzerland), vol. 19, no. 4, 2019, doi: 10.3390/s19040766.

[38] S. Deep, X. Zheng, C. Karmakar, D. Yu, L. G. C. Hamey, and J. Jin, “A Survey on Anomalous Behavior Detection for Elderly Care Using Dense-Sensing Networks,” IEEE Commun. Surv. Tutorials, vol. 22, no. 1, 2020, doi: 10.1109/COMST.2019.2948204.

[39] J. Dahmen, B. L. Thomas, D. J. Cook, and X. Wang, “Activity learning as a foundation for security monitoring in smart homes,” Sensors (Switzerland), vol. 17, no. 4, 2017, doi: 10.3390/s17040737.

[40] CASAS, “CASAS dataset.” [Online]. Available: http://casas.wsu.edu/datasets/.

[41] K. Ramapatruni, S.; Narayanan, S.; Mittal, S.; Joshi, A.; Joshi, “Anomaly Detection Models For Smart Home Security,” 2019.

[42] J. Dahmen, D. J. Cook, X. Wang, and W. Honglei, “Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats,” J. Reliab. Intell. Environ., vol. 3, no. 2, 2017, doi: 10.1007/s40860-017-0035-0.

[43] Y. Bouabdallaoui, Z. Lafhaj, P. Yim, L. Ducoulombier, and B. Bennadji, “Predictive maintenance in building facilities: A machine learning-based approach,” Sensors (Switzerland), vol. 21, no. 4, 2021, doi: 10.3390/s21041044.

[44] Z. Sui, M. Niedermeier, and H. De Meer, “TAI: A Threshold-Based Anonymous Identification Scheme for Demand-Response in Smart Grids,” IEEE Trans. Smart Grid, vol. 9, no. 4, 2018, doi: 10.1109/TSG.2016.2633071.

[45] G. Oguntala, R. Abd-Alhameed, S. Jones, J. Noras, M. Patwary, and J. Rodriguez, “Indoor location identification technologies for real-time IoT-based applications: An inclusive survey,” Computer Science Review, vol. 30. 2018, doi: 10.1016/j.cosrev.2018.09.001.

[46] R. Jadon, A.; Omama, M.; Varshney, A.; Ansari, M.; Sharma, “Firenet: A Specialized Lightweight Fire & Smoke Detection Model For Real-Time Iot Application,” 2019.

[47] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” Journal of Network and Computer Applications, vol. 84. 2017, doi: 10.1016/j.jnca.2017.02.009.

[48] buildingSMART International., “Industry Foundation Classes (IFC) - buildingSMART Technical,” buildingSMART International, 2021. .

[49] T. H. Kolbe, C. Nagel, and A. Stadler, “CityGML – OGC Standard for Photogrammetry ?,” Processing, 2009.

[50] European Big Data Value Association, “European Big Data Value Strategic Research and Innovation,” BigDataValu.eu, no. July, 2014.

[51] E. Commission, “Workshop on advanced and interoperable digital Business-to-business platforms for smart factories and energy - FUTURIUM.” .

[52] F. Foundation, “Smart Energy - FIWARE Foundation Open Source Platform.” .

[53] IDSA, “International Data Spaces | The future of the data economy is here.” .

[54] AIOTI, “AIOTI - The Alliance for the Internet of Things Innovation,” Website, 2018. .

[55] V. Marinakis, T. Koutsellis, A. Nikas, and H. Doukas, “Ai and data democratisation for intelligent energy management,” Energies, vol. 14, no. 14, 2021, doi: 10.3390/en14144341.

[56] V. Marinakis, “Big data for energy management and energy-efficient buildings,” Energies, vol. 13, no. 7, 2020, doi: 10.3390/en13071555.

[57] V. Marinakis et al., “From big data to smart energy services: An application for intelligent energy management,” Futur. Gener. Comput. Syst., vol. 110, 2020, doi: 10.1016/j.future.2018.04.062.

[58] V. Marinakis and H. Doukas, “An advanced IoT-based system for intelligent energy management in buildings,” Sensors (Switzerland), vol. 18, no. 2, 2018, doi: 10.3390/s18020610.

[59] A. Broder and M. Mitzenmacher, “Network applications of bloom filters: A survey,” Internet Math., vol. 1, no. 4, 2004, doi: 10.1080/15427951.2004.10129096.

[60] D. C. Y. Vargas and C. E. P. Salvador, “Smart IoT gateway for heterogeneous devices interoperability,” IEEE Lat. Am. Trans., vol. 14, no. 8, 2016, doi: 10.1109/TLA.2016.7786378.

[61] N. Q. Uy and V. H. Nam, “A comparison of AMQP and MQTT protocols for Internet of Things,” 2019, doi: 10.1109/NICS48868.2019.9023812.

[62] Kafka, “Apache Kafka.” .

[63] MongoDB, “MongoDB: the application data platform.” .

[64] Spark, “Apache SparkTM - Unified Engine for large-scale data analytics.” .

[65] Hadoop, “Apache Hadoop.” .

[66] S. Parikli, D. Dave, R. Patel, and N. Doshi, “Security and privacy issues in cloud, fog and edge computing,” in Procedia Computer Science, 2019, vol. 160, doi: 10.1016/j.procs.2019.11.018.

[67] R. van der Weerdt, V. de Boer, L. Daniele, and B. Nouwt, “Validating SAREF in a Smart Home Environment,” in Communications in Computer and Information Science, 2021, vol. 1355 CCIS, doi: 10.1007/978-3-030-71903-6_4.