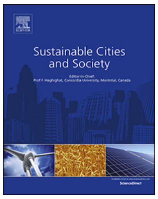
Sustainable Cities and Society 62 (2020) 102370

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs



Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid

Muhammad Babar[a], Muhammad Usman Tariq[b], Mian Ahmad Jan[c,d,*]

[a] *Computing and Technology Department, Iqra University, Islamabad, Pakistan*
[b] *Abu Dhabi School of Management, Sharjah, United Arab Emirates*
[c] *Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City, Viet Nam*
[d] *Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Viet Nam*

ARTICLE INFO

Keywords:
Smart grid
Security
Machine learning
Internet of things
Demand-side management
Home area network

ABSTRACT

The national security, economy, and healthcare heavily rely on the reliable distribution of electricity. The incorporation of communication technologies and sensors in the power structures, recognized as the smart grid which revolutionizes the model of the production, distribution, monitoring, and control of the electricity. To realize the applicability of smart grid, several issues need to be addressed. Securing the smart grid is a very challenging task and a pressing issue. In this article, a secure demand-side management (DSM) engine is proposed using machine learning (ML) for the Internet of Things (IoT)-enabled grid. The proposed DSM engine is responsible to preserve the efficient utilization of energy based on priorities. A specific resilient model is proposed to control intrusions in the smart grid. The resilient agent predicts the dishonest entities using the ML classifier. Advanced energy management and interface controlling agents are proposed to process energy information to optimize energy utilization. The efficient simulation is executed to test the efficiency of the proposed scheme. The analysis results reveal that the projected DSM engine is less vulnerable to the intrusion and effective enough to reduce the power utilization of the smart grid.

1. Introduction

IoT is the next step advancement of today's Internet, where nodes, objects, or things are embedded with communication and computation capabilities (Babar, Arif, Jan, Tan, & Khan, 2019; Din, Paul, Hong, & Seo, 2019). The IoT devices can be seamlessly assimilated to the Internet at various levels (Al-Garadi et al., 2020). The IoT provides foundation for the smart cities services such as smart health, smart transportation, smart home, smart grid, smart surveillance and so forth. One of the biggest systems of IoT is the Smart Grid which is nothing but the conventional grid augmented with the integration of renewable energy and large-scale ICT (Information and Communication Technologies) (Al-Turjman & Abujubbeh, 2019; Khatua et al., 2020). The IoT-based smart appliances can be embedded in the smart grid via all of its main parts such as production, communication, supply, and use (Abujubbeh, Al-Turjman, & Fahrioglu, 2019). The energy necessities of this century are mounting very fast due to the population growth in the societies. The national security, national economy, and the healthcare of the societies heavily rely on the reliable and resilient distribution of electricity. The customary electrical grids are static and inefficient to cope up with the demands of the consumers accordingly. Smart Grid is the next generation of the grid, that is anticipated to transfigure the mode of the production, distribution, and control of the electricity. The smart grid will improve the life of next-generation citizens and will make it sustainable as the consumers of the smart grid are very much active and participating in the system in the form of priorities and demands setting (Ahmad, Zhang, & Yan, 2020). Therefore, various nations have started adopting smart grid services to advance societies. The market of the traditional grid is national and centralized, where the smart grid market is decentralized and ignore the boundaries.

Continuous communication is essential for a smart grid and IoT incorporation can improve it. The smart grid is more efficient than the traditional grid in terms of production, market, transmission, distribution, and consumers (Yan, Qian, Sharif, & Tipper, 2012). The classical grids have limited large power plants while the smart grid has numerous small power producers. The traditional grid transmission is based on large power lines and pipelines where the smart grid includes small scale transmission and regional supply compensation which makes the smart grid much more efficient than the traditional grid. The consumers of the smart grid are very much active and participating in

[*] Corresponding author at: Informetrics Research Group and Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
E-mail addresses: mhammad.babar@iqraisb.edu.pk (M. Babar), m.tariq@adsm.ac.ae (M.U. Tariq), mianjan@tdtu.edu.vn (M.A. Jan).

https://doi.org/10.1016/j.scs.2020.102370
Received 11 May 2020; Received in revised form 28 June 2020; Accepted 30 June 2020
Available online 03 July 2020

the system in the form of priorities and demands set. The market of the traditional grid is national and centralized, where the smart grid market is decentralized and ignore the boundaries. The Smart Grid is considered a critical structure as it is comprised of billions of smart appliances, smart meters, sensors, and so forth along with numerous communication setups whether private or public (Lezama, Soares, Canizes, & Vale, 2020).

However, to realize the applicability of the smart grid, several issues need to be addressed before the realization (Passerini & Tonello, 2019). Security is one of the most severe among the pressing issues and a big biggest challenge to the smart grid (Khan, Asif, Ahmad, Alharbi, & Aljuaid, 2020). A malicious attack on the grid could take overwhelming consequences on the trustworthiness of the extensive structure of the smart grid (Qasaimeh, Turab, & Al-Qassas, 2019; Radoglou-Grammatikis & Sarigiannidis, 2019). Even one particular smart grid node is conceded, the entire grid turns out to be vulnerable. The devices in the offices, homes, and hospitals may be affected due to the shutting down of the entire grid caused by cyber-attacks that could chore the whole city to a pause and it can cause severe financial losses (Weerakkody & Sinopoli, 2019; Yadav, Mahajan, & Thomas, 2018). Therefore, security is considered one of the critical factors before the deployment of large scale IoT-enabled smart grids. Smart grids expose to security including but limited to false data injection, data theft, insider attacks, denial of service (DoS) attacks, energy theft, malware, and so forth. In recent days, safety provisioning in a smart grid is a sophisticated task (Alladi, Chamola, Rodrigues, & Kozlov, 2019; Narayanan, Khanna, Panigrahi, & Joshi, 2019). The cryptography, protected multi-party processing, and differential privacy have come across to solve many security problems (Gope & Sikdar, 2018; Lim, Doh, & Chae, 2017; Sha, Alatrash, & Wang, 2016; Tsai & Lo, 2015). However, these solutions are visible to a generic type of confrontational attacks and they are a shortage of secured features.

Therefore, the security challenges using machine learning are explored in this paper on the IoT-enabled smart grid. This paper proposes a secure and resilient demand-side management (DSM) engine using the Internet of Things (IoT) to overcome the security issue in the smart grid. The proposed DSM engine is equipped with a resilient agent using a ML classifier. A stream processing unit is also integrated with the DSM engine to process the information produced by IoT devices. A specific HAN is designed to realize the proposed DSM to optimize energy utilization

2. Background and literature review

Security and trust in a smart grid based on IoT is a subjective phenomenon that causes difficulty in identifying attacks absence or presence (Kimani, Oduol, & Langat, 2019). The insecure smart grids can cause failure to the services of the smart cities (Habibzadeh, Nussbaum, Anjomshoa, Kantarci, & Soyata, 2019). The IoT-enabled grids construct a multifaceted interrelated network, where a huge capacity of data stored. This data is usually kept on the cloud which is vulnerable to threats and security breaches may occur which a serious concern. The important information in the grid, research data, and the DSM are the key elements that are targeted that is why they are more vulnerable. Therefore, various security proposals have been given in the past. The existing proposals observe communication to identify insecure communication. Nevertheless, it is very difficult to recognize insecure communication in a system that is composed of numerous nodes. i.e., IoT-enabled smart grid. A sound work had been carried out in the security for the smart grid. However, various deficiencies are not addressed in the exiting literature.

An essential instrument for getting insights from the massive quantity of information generated by the IoT nodes in the IoT-enabled smart grid is the Machine Learning (Ahmed, Ahmad, Piccialli, Sangaiah, & Jeon, 2018; Ahmed, Din, Jeon, & Piccialli, 2020; Bhattarai et al., 2019; Hossain, Khan, Un-Noor, Sikander, & Sunny, 2019; Hussain, Hussain, Hassan, & Hossain, 2020). Machine learning methods offer effective means to investigate the information, predict from accessible data, and perform decision-making to run the smart efficiently. ML algorithms can be utilized for the smart grid functionalities including predictions of energy utilization, cost, energy production, optimum time, fault recognition, attack prediction, and uncovering the intruders (Negnevitsky, Mandal, & Srivastava, 2009). The security threats are always crucial for such a system huge system as both supply-side and demand-side of energy sources are affected badly. Arraying a smart grid has unavoidable effects on organization and society that badly affects all the elements of its technical structure. Therefore, safety actions also essential to be likewise pervasive particularly utilizing the machine learning techniques that can be extremely helpful in the smart grid to improve the life of the societies.

Detection and protection can be the two main classes of the security approaches. The protection policies could be administrative and hardware-oriented together with the software safeguards which are most-obvious. The detection can be furnished through ML algorithms that can foresee malicious threats in addition to the identification of irregularities based on the accessible features (Ali, Wu, Weston, & Marinakis, 2015). ML approaches are appropriate in most mutual responsibilities which include regression, classification, and prediction. It is one of the most important favorable solutions to cyber-threats in this era of smart grid and deficient security-defense (Kalogridis, Sooriyabandara, Fan, & Mustafa, 2014). Cyber protection can be achieved at both sides such as consumers and providers. The consumers' side security protection is deployed in smart meters and DSM aspects of the smart grid are made secure by the providers. Few proposals based on machine learning algorithms such as apriori association rules and Bayesian classification, but they considered only one feature for the context-based cyber-attacks (D'Angelo, Rampone, & Palmieri, 2017; Li et al., 2020; Mehmood, Mukherjee, Ahmed, Song, & Malik, 2018).

A hybrid architecture for DSM was proposed utilizing ML algorithms, entropy-enabled feature selection, and soft computing (Jurado, Nebot, Mugica, & Avellana, 2015). The said hybrid approach is totally dependent on the entropy which is a de-merit. In addition, this hybrid approach utilized the soft computing concepts partially and the simulation detail is also missing. Various algorithms were proposed, for instance, support vector regression, extreme learning machine, improved second-order, error correction, and neural network for predicting load in the smart grid. Big data analytics techniques for DSM have also been proposed (Babar & Arif, 2018; Iqbal, Qureshi, Kanwal, & Jeon, 2020). Managing energy dynamically using big data analytics is a promising approach too (Babar, Rahman, Arif, & Jeon, 2018). HAN is one out of three important layers used in the smart grid (Zhu, Lambotharan, Chin, & Fan, 2012) which is comprised of both wireless and wired technologies such as power lines for wired and Bluetooth, ZigBee, and WiFi for wireless (Ahmed et al., 2019; Li et al., 2019). The key element of HAN is a home gateway that gathers data from smart appliances of home.

Hence, to improve the trustworthiness of IoT-enabled smart grid applications, the level of insecurity of a smart appliance need to be asses first. We propose a resilient agent in a secure DSM engine that would be assessing the trust level initially using an ML algorithm. As security differs from one smart appliance to other, context-relevant features are cautiously mined in proposed secure DSM engine.

3. Proposed secure demand side management engine for smart grid

DSM is the most important element of the smart grid where consumers notify the utilities about power consumption and the utilities or producers' response accordingly. The real-time cost is dispatched by power utilities according to consumer demand. The position of the projected secure DSM associated with the smart grid and HANs are depicted in Fig. 1. The HANs are connected to the smart grid which are

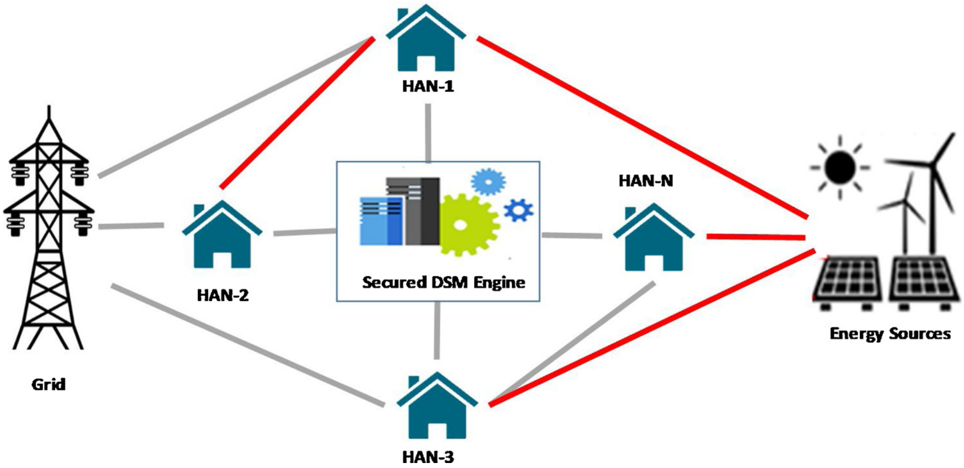


Fig. 1. Position of DSM Engine.

the subsystems devoted to DSM within Smart Grid. It is comprised of demand response and energy proficiency that are the crucial modules in comprehending worth in the deployment of smart grid.

A HAN is used to observe and govern the energy consumption in the home which is a dedicated network. It observers and governs the smart appliances in the context of smart metering. The HAN includes an application that monitors the entire network. The HAN, Home Area Market, and smart homes are now evolving within the smart grid to serve the home services with efficient resource utilization. HAN has high associations for smart grid vendors, as the utilities are looking for means to implement DSM programs. The secure DSM engine in a smart grid is used to maintain efficient energy utilization in a secure way which is based on priorities and demands of energy. The high energy demand and prioritized devices are selected and served timely within the specified constraints or parameters of load and cost limits along with authentication. The system model of the proposed secure DSM engine is shown in Fig. 2. The proposed model solution is not available commercially.

The IoT-enabled HAN are the data sources for the proposed secure DSM engine. The data is received by the message receiver in the DSM engine where the authentication is performed to secure the message from intruders. The secured data is then processed for the decision-making according to the demand and priorities of the consumers in the smart grid. The results of the processing data are sent to the HAN again for efficient resource utilization. The results may also be utilized for trend analysis for future prediction.

3.1. Resilient agent

The proposed architecture has a resilient agent for securing the grid from malicious attacks. It resides within DSM connected to HANs and grid to secure the communication for both consumers and providers and offers resilience against the cyber-attack by recognizing the malicious units. The provider manager (PM), consumer manager (CM), and monitoring analyst (MA) are the elements of a resilient agent. The PM and CM are basically the mangers who manages the security elements in the proposed resilient agent. The PM and CM take care of the providers and consumers while the AM is used to apply the machine learning (ML) algorithm. The Naïve Bayes ML algorithm utilized in the proposed resilient agent which classifies the communication as secure or insecure. The Naïve Bayes is preferred because it performs better compared to other algorithms when supposition of independent predictors becomes true.

The PM is responsible for maintaining the profiles of every provider. The profile may contain information such as identification, abilities, level of trust, etc. The CM is responsible for maintaining the profiles of every consumer. The CM functioning is based on various attributes including identification and level of trust which support in recognizing dishonest and honest consumers. The Monitoring Analyst of a resilient agent in the proposed DSM engine uninterruptedly observes the communication. It splits the fraudulent entities of communicating from truthful one by classifying different attacks. The MA is trained using the Naive Bayes ML algorithm. Though, categorization and scaling of features are performed before training.

The proposed resilient agent based on Naïve Bayes algorithms is used to predict the level of security using 5 different classes that are fully secure, good secure, fairly secure, full insecure, partially insecure. Eq. (1) is used to calculate the score of security.

$$SecLevel = \begin{cases} Full\ Secure, & if\ S = 1 \\ Good\ Secure, & if\ S \geq 0.76\, and\, S < 1 \\ Fairly\ Secure, & if\ S \geq\ 0.51\, and\, S < 0.76 \\ Partially\ InSecure, & if\ S \geq 0.26\, and\, S < 0.51 \\ Full\ InSecure, & if\ S = 0\, and\, S < 0.26 \end{cases} \tag{1}$$

Where S is calculated using Eq. (2).

$$S = \frac{1}{n}\sum_{k=0}^{n} Fk \tag{2}$$

where the average of F for all the features of is computed after its utilization.

3.2. Advance energy management agent

In addition to the resilient agent the proposed DSM engine provides core functionalities of efficient energy management. A specific unit Advance Energy Management Agent is proposed (AEMA) to manage efficient energy utilization. The main goal of the proposed AEMS component is to satisfy consumer energy demands while preserving energy efficiency. The AEMS contribution is to achieve the efficient resource utilization particularly better energy utilization. AEMA constitutes two main parts 1) ZigBee sensor supported electrical devices controlling system and 2) lighting control system supported by light sensor exploits natural illumination.

In fact, energy utilization strictly relies on the activities of residential habitat within the home environment. Henceforth, operations are executed in a semi-automated manner, which is initiated by users and controlled by the AEMA. The management station sends control commands to turn off an appliance after switched on with user input. Time of operation is a key parameter of computing energy consumption. Upon receiving switch on requests from a user, time is saved at the controlling station. Since appliance controlling is based on user

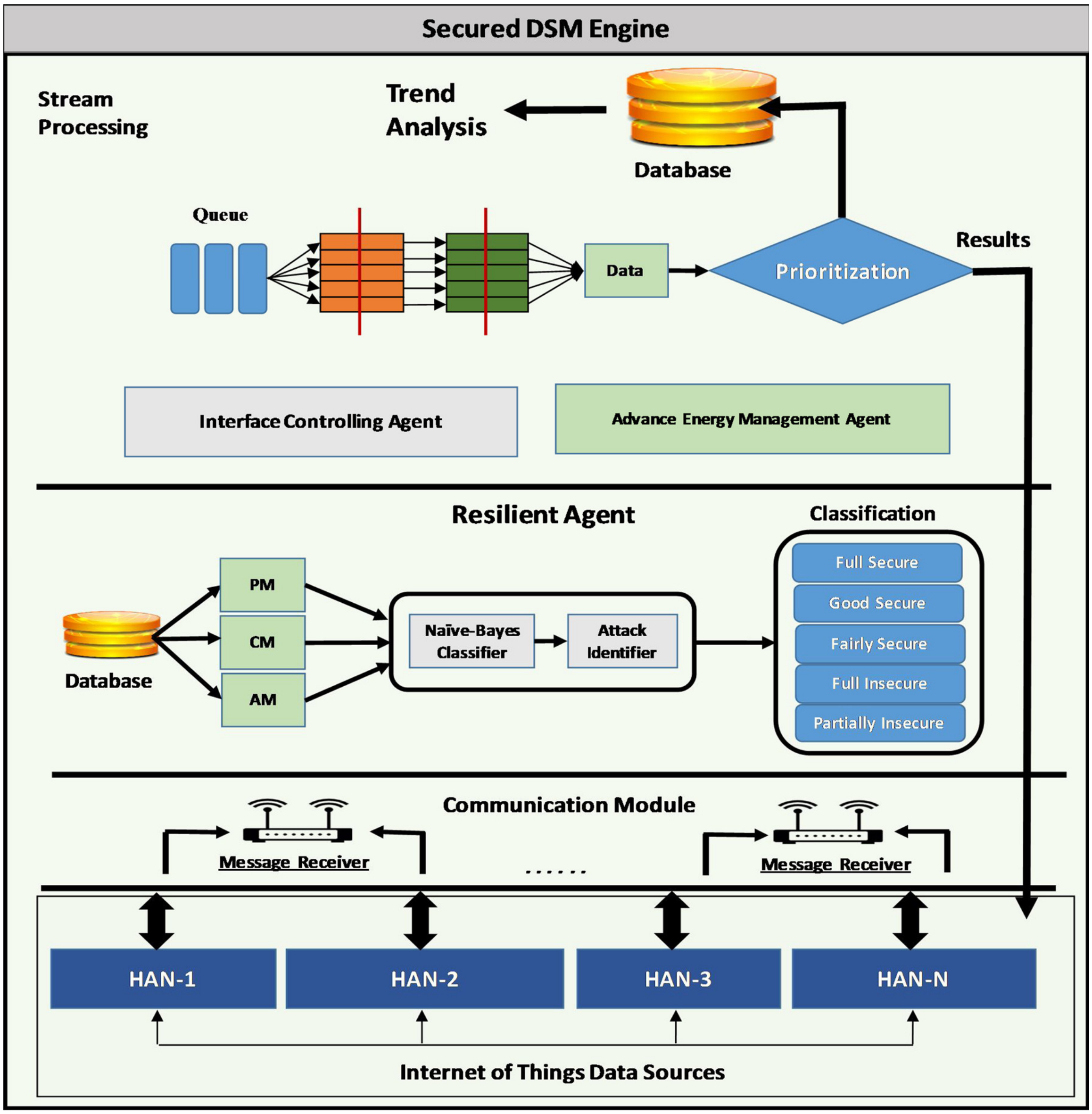


Fig. 2. System Model.

behaviors, the incidence of a user is checked from time to time. If user absence is detected during these periodic checks, all appliances that are turned on will be turned off by AEMA to minimize energy wastage. At the same time, the management station updates device switched off time. In order to uniquely identify the appliances for controlling purposes, each electrical device is attached with a sensor of ZigBee. Each sensor is assigned with an identification number that allows distinguishing among other sensors in the smart home network. In particular, appliance controlling should not interfere with consumer satisfaction levels. Therefore, an event handling unit is embedded in the management station to provide communication between the management station and home users.

The proposed AEMA in DSM engine offers a control system to minimize the energy. The DSM control system adjusts the luminance level of light of the different smart appliances of HAN based on the area occupied by the sunlight. We defined a situation parameter and identified four various scenarios according to the angle of the sunlight. The DSM control system calculates the required luminance level of the light source on the basis of intensity acquired from the light sensor. Following relation is used to compute the intensity () for the light controlling system.

$$I_{\theta_i} = \begin{cases} \varphi\left[\frac{1}{2}(b1 \times h1) + (b2 \times x)\right] \pm \delta & 0^{\circ} \leq \theta_1 < 15^{\circ} \\ \frac{\varphi}{2}[(b3 \times h2) + (b4 \times h3)] \pm \delta & 15^{\circ} \leq \theta_2 < 30^{\circ} \\ \varphi\left[\frac{1}{2}(b6 \times x) + (b5 \times x)\right] \pm \delta & 30^{\circ} \leq \theta_3 < 45^{\circ} \\ \varphi\left[\frac{1}{2}(b6 \times x) + (b5 \times x)\right] \pm \delta & 45^{\circ} \leq \theta_4 < 60^{\circ} \\ \varphi x^2 & \textit{Otherwise} \end{cases} \tag{3}$$

The Control system is responsible to control the intensity of the light considering environmental factors as well. A tuning factor is introduced for this intensity control. The intensity is represented by which is calculated by using Eq. (4).

$$\varphi = \frac{FL_x \times L_M \times R_f}{\Gamma} \tag{4}$$

Where FL_x is the entire luminous by a source, L_M is the lumen, R_f is the lampshade echo constant, and Γ is the source length.

Table 1
DSM Parameters.

Parameter	Description
Device-Load	Load mandatory to make operational a particular node.
Cost	It the correlation of the demand and time. It could vary at various time which is a serious factor from consumer perspective in the smart grid.
Load Limit	Commonly, this is a specific limit which is quantified by the providers. It might vary according to end user tariffs and hours. It is a serious factor from supplier perspective.
Time	The load and the cost is measured in the context of time. Therefore, it is the deciding factor for several other parameters
Device Priority	The priority of a particular device may vary with time. It is the degree of importance or use at specific time. A node may have one of the following priorities at a time which may dynamically according to situation. The priorities are classified into Real Time, High, Medium, Low, Not Required.

Table 2
Device Priority.

Priority	Description
Real Time	The device is unavoidable at all and must needed irrespective of limits of cost and load or trade-offs.
High	The demand of the node is very extraordinary while being in the cost but not load.
Medium	If it is feasible for the device to remain in the cost and load limits, then it is required otherwise constrained are put.
Low	The device can be shut down for other prioritized devices and has low priority.
Not Compulsory	The node will shut down until significance is altered

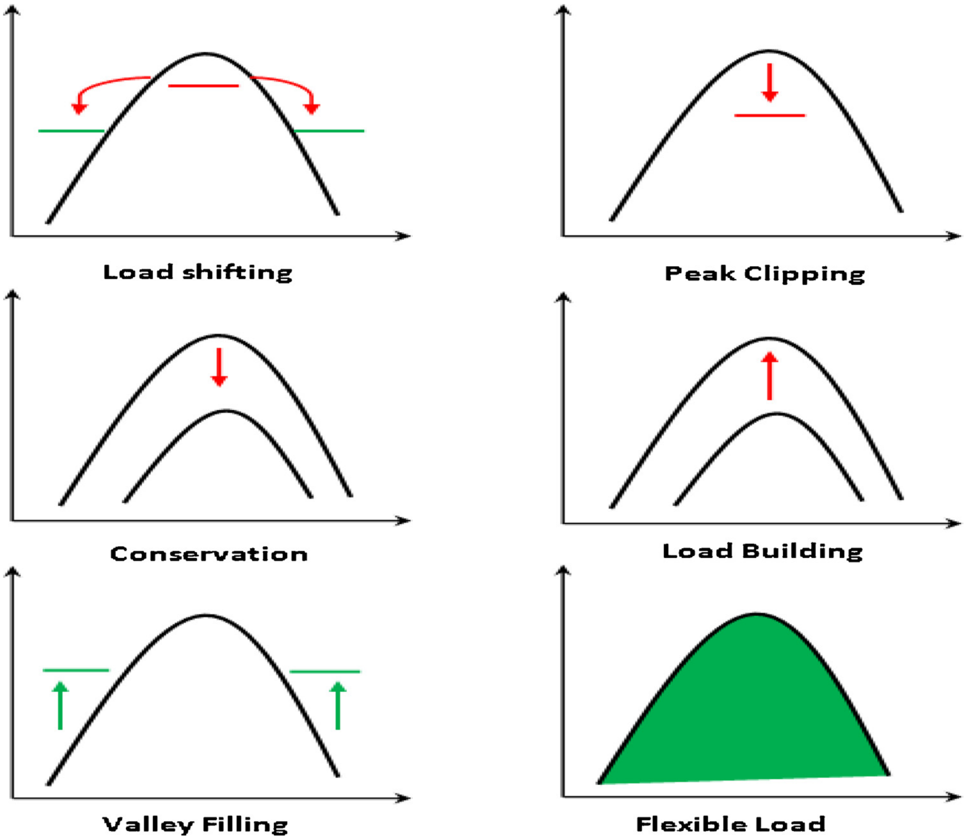


Fig. 3. DSM Techniques.

3.3. Interface controlling agent

Interface Controlling Agent (ICA) is evident from the previous studies, the synchronicity of manifold wireless equipment degrades the efficiency of one another. The ICA is preferred due to the synchronicity to better control the interfaces. This aspect was the motivation behind the proposed ICA. The smart home network consists of both WLAN and ZigBee WSN. These technologies operate on the 2.4 GHz ISM band and, thus leads to coexistence interference. Therefore, we can claim that interference is highly influenced by the distance between nodes and the Wi-Fi access point (AP). Henceforth, the distance factor is considered when designing the solution to minimize the adverse effects of interference. Direct communication or relay node based communication is highly favored in traditional WMNs, which on the other hand leads to a significant increase in packet loss. Another key point to consider is packet loss rate increases with the distance to be traveled, in order to reach the destination. In other words, all these possibilities create a negative influence on the success rate of data transmission that consequently reflects on performance degradation of smart home appliances and devices.

Thus, ZigBee coordinators are introduced into this architecture. The responsibility of coordinators is to minimize packet loss resultant from

Table 3
DSM Techniques Description.

Priority	Description
Load Shifting	It is used to isolate the devices according to their priority. Few devices must be switched off as it keeps on high priority devices and low priority devices shift to other suitable time.
Peak Clipping	This technique is familiar to control the load and diminish the peak load for optimum level.
Conservation	It is utilized to reduce the consumption of the energy
Load Balancing	This method balances the load of the energy in the grid and overall system
Valley-Filling	It straight rises the load in off-peak time and is the reverse of peak-clipping.
Flexible-Load	This method offers the flexibility to provide flexible solution of energy

The consumers are required to have some trade-offs to realize the desire results which are described in Table 4.

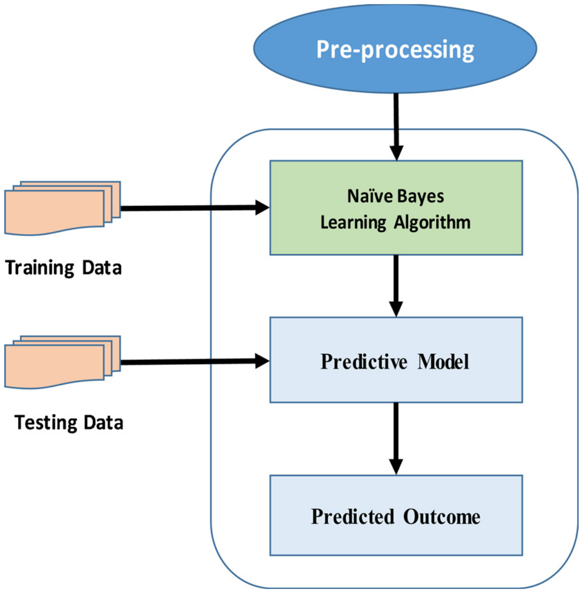


Fig. 4. Model Training.

coexistence interference and distance between sensor nodes and a management station. Each room of the house and kitchen is equipped with a ZigBee coordinator. Since physical distance is a vital factor for interference, the appropriate placement of the ZigBee coordinator guarantees minimal interference on the same band. Moreover, it reduces the number of hops between source and destination, which eventually minimizes the packet loss.

Considering the distance between sensor and Wi-Fi AP, all sensor nodes in the smart home are divided to n groups. The space connecting Wi-Fi AP and sensors was taken into account, since the proposed scheme considers the coexistence interference ZigBee WSN and WLAN. The set of sensors in the closest proximity belong to group 1 (G_1). The sensors in G_1 adheres to distance threshold ($d[\sigma_1]$), where distance (d) is less than the threshold, $d < d[\sigma_1]$. In a similar way, rest of the sensor nodes are grouped into $G_2 \ldots G_n$, respectively follows an increasing distance threshold $d[\sigma_2] < d[\sigma_3] \ldots d[\sigma_n]$. The sensors in G_1 suffer with highest rate of interference as a result of closeness to Wi-Fi AP. When a ZigBee channel is occupied for WLAN communication, generally it increases the tendency that adjacent channels to be occupied by WLAN signals. Hence, we assign a set of channels to each group G to overcome the consequences of afore stated phenomenon. For the sensors in G_1, non-overlapping channels are assigned as they are the closest group of sensors to Wi-Fi AP. From G_2 to G_n channel are assigned based on the decisions made according to MADM model. MADM technique in this scenario occupies a criterion (c) that comprises with bandwidth, quality, and occupancy. Channel assignment based on MADM is carried out in 5 steps as outlined below.

I Classify and normalize the criteria into a decision matrix
II Construct the weighted decision matrix
III Compute for both positive ideal situation and negative ideal situation
IV Compute the segregation between positive and negative ideal situations
V Compute the ranks of available channels

For each criterion, weight (w) is assigned as $w_x = c_x / \sum_{x=2}^{y} c_x$. Consequent to the rank computation, channels are arranged in the ascending order. The groups closer to Wi-Fi AP are assigned with channels that have obtained higher ranks and vice versa. Eventually, ICS ensures uninterrupted seamless communication within the home network that consists with heterogeneous wireless technologies.

3.4. Techniques, parameters and trade-offs for DSM engine

After the authentication of the data and messages, the DSM is responsible to maintain the efficient energy utilization based on priorities and demands of energy. The efficient energy utilization is performed on the basis of parameters which affect the smart grid performance, techniques selection based on requirement and priorities, and the trade-off of consumers. The list of effecting parameters or constraints are for the smart grid are also described in Table 1.

The last parameter of the DSM is the Device Priority. These priorities are described in Table 2. The parameters are affecting the DSM techniques and vice versa. The DSM techniques affecting parameters are strongly associated with better trade-offs decisions.

The methods depicted in Fig. 3 are used to achieve the goal of the DSM to persist in cost and load limits. The load is the primary concern form provider's view of secondary concern from the consumer's view. These techniques of DS Mare also described in Table 3.

Table 4
DSM Trade-offs.

Trade-offs	Description
Availability vs. Cost	The more availability means high cost. It is the decision of consumer to prefer cost of availability of the energy.
Availability vs. Load	The load is increased if availability is preferred. If the availability is demanded by the consumer, then it is provider's offer the required load. It is achieved with smart grid alternate foundations of power.
Load vs. Cost	The more load means high cost, but in some cases the cost might decrease in off-peak time. The DSM technique must be equipped to select optimum values if trade-offs are not preferred by consumers

Table 5
Confusion Matrix.

	Predicted		
		Secure	Insecure
Actual	Secure	TP	FN
	Insecure	FP	TN

Table 6
Proposed Model Results using Confusion Matrix.

	Predicted		
		Secure	Insecure
Actual	Secure	94 %	6 %
	Insecure	7 %	93 %

4. Results and discussion

The comprehensive exploration and debate of results achieved using the proposed model discuss in this part. The efficacy of the resilient DSM engine proposed is revealed with a specially premeditated simulated setting.

Two sets of trials were carried out which are

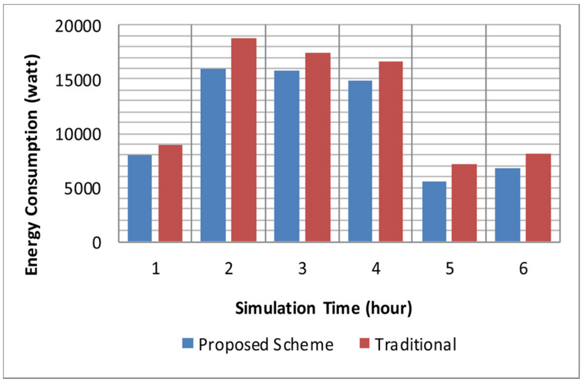
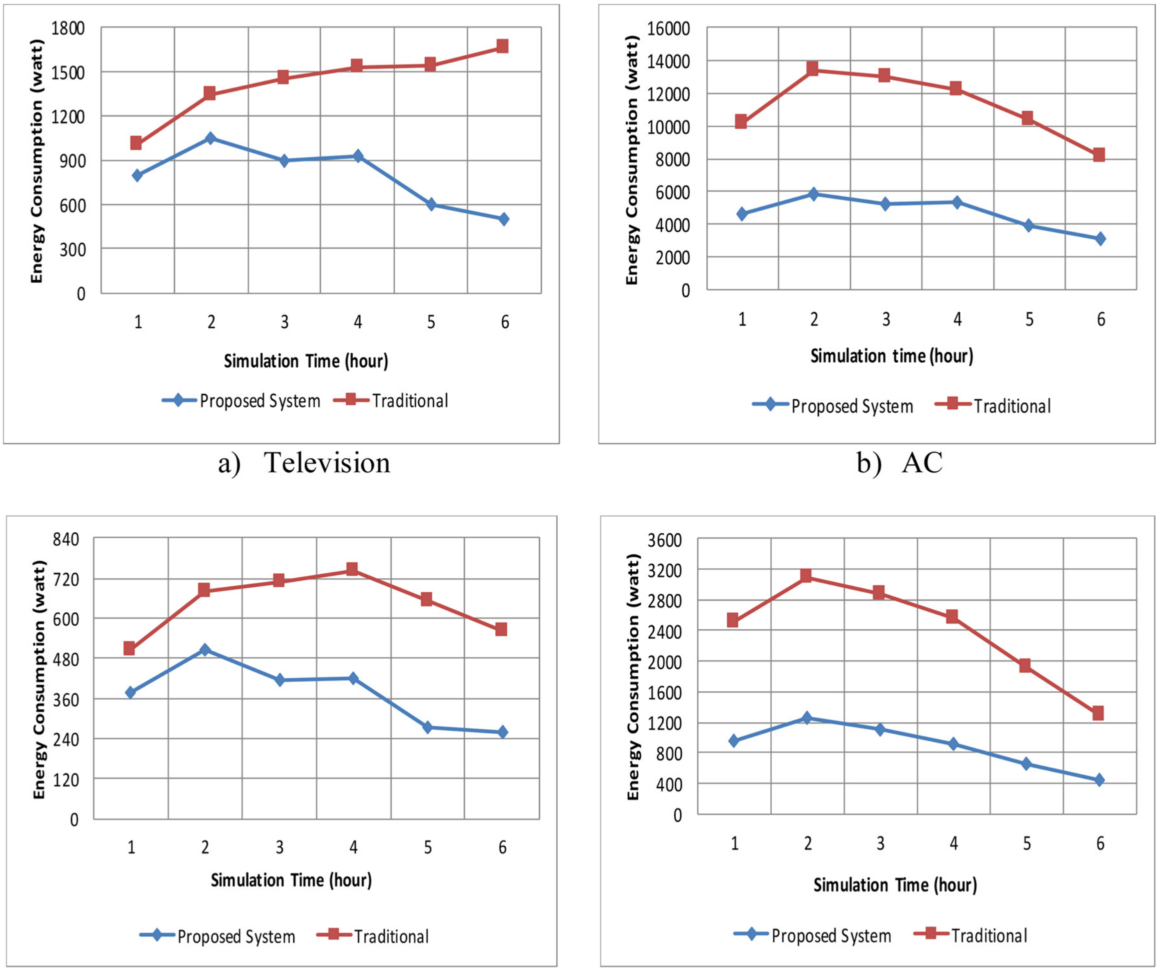


Fig. 6. Energy Consumption of other nodes.

1 Experiments of the resilient engine using Naïve Bayes algorithms including the training of the model. The specific reliable and authentic dataset is used to train the model to differentiate between secure and insecure communication entities or things (WS-Dream Team, 2018).
2 The energy efficiency evaluation of the overall DSM engine for different scenarios where a specific HAN with fixed WIFI APs using the C# high-level programming. The stream processing is also carried out on a reliable dataset.

The resilient agent evaluation is carried out by designing a specific environment. In the beginning, the proposed resilient agent was trained



a) Television

b) AC

c) Fan

d) Refrigerator

Fig. 5. Energy Efficiency of Proposed DSM Engine.

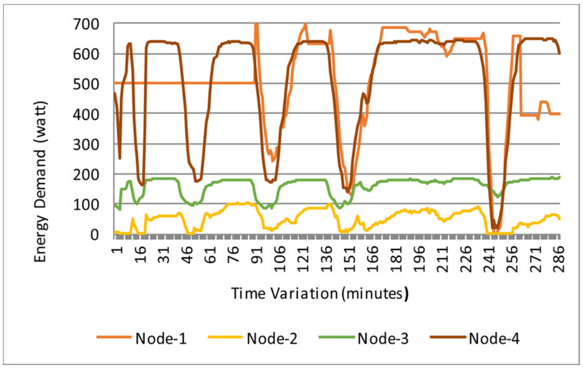


Fig. 7. Energy Demand of Nodes.

using the classifier on 340*900 matrix that is the assessment of the 900 services by 340 consumers. The Naive Bayes algorithms perform on the hypothesis that a feature existing in one class will not be a part of other features. The training of the Naïve Bayes classifier is depicted in Fig. 4.

To measure the efficiency of a resilient agent proposed classifier, the confusion matrix is utilized as shown in Table 5. The accuracy is evaluated in the context of two classes which are secure and insecure. The confusion matrix is preferred because it can give a better impression of classification model. In addition, it is most widely used performance measurement technique for machine learning algorithms.

The secure is considered if the S value is greater than or equal to 0.51 and less than or equal to 0.5 is considered insecure. These terminologies are considered as they are taken into consideration in the previous proposals. The proposed model results are shown in Table 6. The detail of the confusion matrix terms is as follow:

- The TP is the set of values where secure communication is classified secure by the proposed resilient agent which is 94 % using the proposed model.
- The TN is those set of values where secure communication is classified as insecure by the proposed resilient agent which is 6% using the proposed model.
- The FP is the set of values where the insecure communication is classified secure by the proposed resilient agent which is 7% using the proposed model.
- The TN is those set of values where the insecure communication is classified as secure by the proposed resilient agent which is 93 % using the proposed model

The proposed architecture power efficiency is evaluated for different scenarios. We use the C# high-level programming language to measure the efficiency of the DSM. We designed a specific HAN with fixed WIFI APs. HAN simulations is preferred because the HANs permits the Grid applications to interconnect intelligently. It is because of the centralized access provision by HAN to multiple devices and appliances. In addition, it also has a proactive mechanism to energy savings.

The users are performing two functions which are randomly turn off and on an IoT appliance for 5 h and constantly generating traffic with a particular series energy (1001–5001 bytes). The energy consumption of IoT sensors and devices are calculated by keeping the user functionality into consideration as random variable i.e., 6–35 seconds. To be more practical, the simulation time is altered to $5-15$ min for the burner. Furthermore, we set up different light sources in a various room with FL, LM, RF, and 0 of 1799 lm, 70 %, 2.21 and 329 mm, respectively. Size of the room is considered to 3100 mm. The user stays for $6-12$ min in one specific room while arbitrarily turning off and on the Internet of things appliances in room.

The utilization of energy consumption of IoT-enabled smart appliances such as AP-1, AP-2, AP-3, and AP-4 is evaluated using proposed and traditional scheme as shown in Fig. 5(a)–(d) correspondingly. The power consumption of the smart appliances is considerably decreased using the DSM engine. Besides, the use is managing and monitoring the smart appliances energy consumption utilization by inspection histories. The main parameters which are considered are the priority and demand of the user. The proposed DSM engine integrated with HAN performs the appliances turning on and off based on the user demand and priorities to save the unsuitable energy use.

Moreover, the trend analysis can also be performed using the recorded information in the DSM. Henceforth, a user is capable to have the favorable utilization of power of the appliances. Similarly, the power utilization of the light source of a room is shown in Fig. 6. The energy consumption is reduced using the proposed approach due to Advance Energy Management which manages efficient energy utilization. Moreover, the energy demand of various nodes at different time is also shown in Fig. 7.

5. Conclusion

The incorporation of communication technologies and sensors in the power structures, recognized as the smart grid. Security is one of the most severe among these pressing issues and it is one of the biggest challenges to the smart grid. In this article, a secure and resilient demand side management (DSM) engine is proposed using machine learning to secure the IoT-enabled smart grid from the malicious attacks. The DSM is responsible to maintain the efficient energy utilization based on priorities and demands. A specific resilient agent model is proposed and equipped with the DSM of smart grid to control intrusions. The resilient agent predicts the dishonest entities using ML classifier. A processing module is also proposed in the DSM engine to process the energy information generated by IoT-enabled HAN (Home Area Network) to optimize the energy utilization. The efficient simulation is also executed to test the efficiency of the proposed scheme. A specific HAN is designed with fixed WIFI. The analysis results reveals that the projected DSM engine is less vulnerable to the intrusion and effective enough to reduce the power utilization of DSM in smart grid and its connected HAN devices.

Declaration of Competing Interest

It is stated that there is NO conflict of interest.

References

Abujubbeh, M., Al-Turjman, F., & Fahrioglu, M. (2019). Software-defined wireless sensor networks in smart grids: An overview. *Sustainable Cities and Society*Article 101754.

Ahmad, T., Zhang, H., & Yan, B. (2020). A review on renewable energy and electricity requirement forecasting models for smart grid and buildings. *Sustainable Cities and Society*Article 102052.

Ahmed, I., Ahmad, A., Piccialli, F., Sangaiah, A. K., & Jeon, G. (2018). A robust features based person tracker for overhead views in industrial environment. *IEEE Internet of Things Journal, 5*(June (3)), 1598–1605.

Ahmed, I., Ahmad, M., Nawaz, M., Haseeb, K., Khan, S., & Jeon, G. (2019). Efficient top view person detector using point based transformations and lookup table. *Computer Communications, 147*(November), 188–197.

Ahmed, I., Din, S., Jeon, G., & Piccialli, F. (2020). Exploring deep learning models for overhead view multiple object detection. *accepted in IEEE Internet of Things Journal* (ISSN: 2327-4662).

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*.

Ali, S., Wu, K., Weston, K., & Marinakis, D. (2015). A machine learning approach to meter placement for power quality estimation in smart grid. *IEEE Transactions on Smart Grid, 7*(3), 1552–1561.

Alladi, T., Chamola, V., Rodrigues, J. J., & Kozlov, S. A. (2019). Blockchain in smart grids: A review on different use cases. *Sensors, 19.22*, 4862.

Al-Turjman, F., & Abujubbeh, M. (2019). IoT-enabled smart grid via SM: An overview. *Future Generation Computer Systems, 96*, 579–590.

Babar, M., & Arif, F. (2018). Real-time data processing scheme using big data analytics in internet of things based smart transportation environment. *Journal of Ambient Intelligence and Humanized Computing,* 1–11.

Babar, M., Rahman, A., Arif, F., & Jeon, G. (2018). Energy-harvesting based on internet of things and big data analytics for smart health monitoring. *Sustainable Computing*

Informatics and Systems, 20, 155–164.

Babar, M., Arif, F., Jan, M. A., Tan, Z., & Khan, F. (2019). Urban data management system: Towards Big Data analytics for Internet of Things based smart urban environment using customized Hadoop. *Future Generation Computer Systems, 96*, 398–409.

Bhattarai, B. P., Paudyal, S., Luo, Y., Mohanpurkar, M., Cheung, K., Tonkoski, R., ... Manic, M. (2019). Big data analytics in smart grids: State-of-the-art, challenges, opportunities, and future directions. *IET Smart Grid, 2*(2), 141–154.

D'Angelo, G., Rampone, S., & Palmieri, F. (2017). Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification. *Soft Computing, 21*(21), 6297–6315.

Din, S., Paul, A., Hong, W. H., & Seo, H. (2019). Constrained application for mobility management using embedded devices in the Internet of Things based urban planning in smart cities. *Sustainable Cities and Society, 44*, 144–151.

Gope, P., & Sikdar, B. (2018). Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Transactions on Smart Grid, 10*(4), 3953–3962.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*. https://doi.org/10.1109/COMST.2020.2986444.

Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access, 7*, 13960–13988.

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: current solutions and future challenges. *IEEE Communications Surveys & Tutorials*.

Iqbal, S., Qureshi, K. N., Kanwal, N., & Jeon, G. (2020). Collaborative energy efficient zone based routing protocol for multi-hop internet of things. *online published in Emerging Telecommunications Technologies* (ISSN 2161-3915).

Jurado, S., Nebot, Á., Mugica, F., & Avellana, N. (2015). Hybrid methodologies for electricity load forecasting: Entropy-based feature selection with machine learning and soft computing techniques. *Energy, 86*(June), 276–291.

Kalogridis, G., Sooriyabandara, M., Fan, Z., & Mustafa, M. A. (2014). Toward uni_ed security and privacy protection for smart meter networks. *IEEE System Journal, 8*(June (2)), 641–654.

Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., Aljuaid, H., et al. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*Article 102018.

Khatua, P. K., Ramachandaramurthy, V. K., Kasinathan, P., Yong, J. Y., Pasupuleti, J., & Rajagopalan, A. (2020). Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues. *Sustainable Cities and Society, 53*, Article 101957.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36–49.

Lezama, F., Soares, J., Canizes, B., & Vale, Z. (2020). Flexibility management model of home appliances to support DSO requests in smart grids. *Sustainable Cities and Society, 55*, Article 102048.

Li, B., Peng, Z., Hou, P., He, M., Anisetti, M., & Jeon, G. (2019). Reliability and capability based computation offloading strategy for vehicular ad hoc clouds. *Journal of Cloud Computing, 8*(December (21)), 1–14.

Li, X., Huang, M., Liu, Y., Menon, V. G., Paul, A., & Ding, Z. (2020). *I/Q imbalance aware nonlinear wireless-powered relaying of B5G networks: Security and reliability analysis.* arXiv preprint arXiv:2006.03902arXiv.

Lim, J., Doh, I., & Chae, K. (2017). Secure and structured IoT smart grid system management. *International Journal of Web and Grid Services, 13*(2), 170–185.

Mehmood, A., Mukherjee, M., Ahmed, S. H., Song, H., & Malik, K. M. (2018). NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. *The Journal of Supercomputing, 74*(10), 5156–5170.

Narayanan, S. N., Khanna, K., Panigrahi, B. K., & Joshi, A. (2019). *Security in smart cyber-physical systems: A case study on smart grids and smart cars." Smart Cities Cybersecurity and Privacy.* Elsevier147–163.

Negnevitsky, M., Mandal, P., & Srivastava, A. K. (2009). Machine learning applications for load, price and wind power prediction in power systems. In: *Proc. 15th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP),* 1–6.

Passerini, F., & Tonello, A. M. (2019). Smart grid monitoring using power line modems: Anomaly detection and localization. *IEEE Transactions on Smart Grid, 10*(6), 6178–6186.

Qasaimeh, M., Turab, R., & Al-Qassas, R. S. (2019). Authentication techniques in smart grid: A systematic review. *Telkomnika, 17*(3), 1584–1594.

Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2019). Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access, 7*, 46595–46620.

Sha, K., Alatrash, N., & Wang, Z. (2016). A secure and efficient framework to read isolated smart grid devices. *IEEE Transactions on Smart Grid, 8.6*, 2519–2531.

Tsai, J.-L., & Lo, N.-W. (2015). Secure anonymous key distribution scheme for smart grid. *IEEE Transactions on Smart Grid, 7*(2), 906–914.

Weerakkody, S., & Sinopoli, B. (2019). *Challenges and opportunities: Cyber-physical security in the smart grid. Smart grid control*. Cham: Springer257–273.

WS-Dream Team (2018). *Towards open source Datasets.* [Online]. Available:http://wsdream.github.io/.

Yadav, D., Mahajan, A. R., & Thomas, A. (2018). Security risk analysis approach for smart grid. *International Journal of Smart Grid and Green Communications, 1.3*, 206–215.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys & Tutorials, 15.1*, 5–20.

Zhu, Z., Lambotharan, S., Chin, W. H., & Fan, Z. (2012). Overview of demand management in smart grid and enabling wireless communication technologies. *IEEE Wireless Communications Letters, 19*(June (3)), 48–56.