Microprocessors and Microsystems 83 (2021) 103954

Contents lists available at ScienceDirect

Microprocessors and Microsystems

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

A smart grid incorporated with ML and IoT for a secure management system

S.C. Dharmadhikari [a], Veerraju Gampala [b], Ch. Mallikarjuna Rao [c], Syed Khasim [d], Shafali Jain [e], R. Bhaskaran [f,*]

[a] Department of Information Technology, Pune Institute of Computer Technology, Pune, India
[b] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh 522502, India
[c] Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad 500090, Telangana State, India
[d] Computer Science & Engineering, Dr.Samuel George Institute of Engineering & Technology, Markapur, Andhra Pradesh, India
[e] Department of Electrical and Electronics Engineering, Sagar Institute of Research and Technology, Bhopal 462041, M.P., India
[f] Department of Information Technology, PSNA College of Engineering and Technology, Dindigul 624622, Tamilnadu, India

ARTICLE INFO

Keywords:
Demand side management (DSM)
Machine learning (ML)
Smart grid (SG)
Internet of Things (IoT)
Home area network (HAN)

ABSTRACT

The economy, national safety, and health care are tremendously dependent on the faithful supply of power. The communication technology integration and sensors in power systems have been authorized as a smart grid (SG) that is revolutionizing the model of power generation, distribution, monitoring, and control. To know the Smart Grid compatibility, many problems are required to be directed. The safety of the smart grid is the most challenging function and very crucial difficulties. This paper proposed, a safe demand-side management machine deploying machine learning for the Internet of Things authorized phase is recommended. The propounded demand-side management (DSM) machine protects the effective energy use based on their preferences. A particular flexibility sample was proposed to manage incursion into the smart grid. Anelastic agent prognosticates swindling companies, the ML classifiers are utilized. Promoted power management and intermediate control companies are recommended for processing power data to improve energy usage. The proposed project's effective simulation is implemented to examine the efficiency. The outcome of the analysis discloses that the planned demand-side management (DSM) machine is less susceptible to the incursion and it is sufficient to decrease the smart grid's energy consumption.

1. Introduction

In today's internet, IoT is the upcoming stride development. Where nodes, communication sets the objects, or things, and computational abilities [1-2]. Internet of Things (IoT) gadgets can integrate seamlessly with the network at different stages [3]. Internet of Things (IoT) gives the basement for Smart City supports for instance Smart Health, Smart Transport, Smart Home, SG, and Smart Tracking, etc. One of IoT's largest systems is the Smart Grid, which is nothing more than a regular grid magnified by a combination of naturally replenished renewable sources of power and large-scale information and communication technologies [4-5]. The smart devices based on IoT can be embedded with the SG in all key areas for example manufacturing, communications, delivery, and application [6]. The energy needs of this hundredth of years are increasing most rapidly because of population density extensions on the communities. The national economy, national security, and the health care of communities rely tremendously **upo**n journal front-end sources for reliable and flexible power supply. Regular power grids, which are stable and ineffective to meet the requests of the customer. SG is the upcoming generation of the grid. The SG can make the upcoming generation's better performances of citizens and create it stable as SG's customer become more spirited and participated in the system. By the preferences and request system forms [7]. Therefore, different countries have initiated accepting SG helps to improve communities. The conventional network market is public and brought together, where the SG market is decentralized and rises above limits. Constant correspondence is fundamental to the SG and IoT joining can maintain it.

The SG is more effective, when compared with the conventional griddle to production, market, exchange, distribution, and consumer

* Corresponding author.
E-mail address: chmksharma@yahoo.com (Ch.M. Rao).

https://doi.org/10.1016/j.micpro.2021.103954
Received 22 November 2020; Received in revised form 4 January 2021; Accepted 8 January 2021
Available online 11 January 2021

[8]. In the classical phase, there are fewer power plants, in the smart phase, there are plenty of smaller power generators. Traditional phase transference is dependent on the high energy connections and conduit, where the SG in that small scale transmission and regional distribution repayment, it creates the smart phase highly effective when compared to the conventional grid. The SG consumers are highly active and participated in the organization, which is in the form of priorities and demands. The conventional grid marketing is national and centralized, where the smart grid market is decentralized and transcends boundaries. Consider there is an important framework because it includes a billion Sensors, Smart meters, smart devices, and more communication systems, private or public [9].To understand the SG compatibility, many problems necessity was considered prior it can be realized [10]. Security in stress issues is very serious and a great challenge to the SG [11]. The malicious outbreak on the grid can have a major impact on the reliability of the comprehensive architecture of the smart grid [12-13]. Even a specific SG node is acknowledged, making the whole grid is vulnerable. The cyber-attack causes the closing of whole grids, which can damage devices in offices, houses, and hospitals, and also it can paralyze the whole city and cause severe financial losses [14-15]. Thus, safety is taken as one of the most important characteristics previously using high-scale IoT-enabled SG. this was included but these are minimized to inaccurate information injection, information theft, internal attacks, DoS attacks, power theft, and malware. Nowadays, providing security in the smart phase is a sophisticated task [16-17]. Protected multi-party processing, cryptography, and various privacy issues have come to sort-out lots of safety issues [18]. However, these solutions are known for a common type of conflict attack, which is the lack of safety features. Therefore, safety challenges using ML are explored in this project on the IoT generated SG. This proposed article a safe and flexible DSM machine utilizing the IoT to tackle safety issues at SG. The propounded demand-side management (DSM) machine is fitted with a flexible agent deploying machine learning classifiers. The particular home area network (HAN) is structured to understand the propounded demand-side management (DSM) to improve power usage.

2. Literature review

Fatima Hussain, et al. have proposed IoT-empowered frameworks structure a versatile interconnected organization, where a large amount of information is saved. This information is typically kept in the cloud and it is powerless against dangers and safety penetrates, which is a significant study. Thus, different safety proposals are provided in the past. Current programs focus on communications to recognize unsafe communications. However, it is so hard to identify unsafe communications with multiple nodes. That is IoT-enabled SG. Sound work was executed in defense for the SG. So that, different drawbacks in the current literature have not been resolved. Machine learning is an important tool for gaining insights from the heavy amount of data's produces internet of things (IoT) node on the internet of things (IoT) -enabled SG.

Tolgasoyata, et al. was presented the conceptual mesh network of smart devices (called "smart boxes"), it can harvest its power from off-grid sources and function in two modes: In normal mode, smart boxes act as information collection gadgets and operate the information through traditional information technology supports, Also provides a comprehensive research map to understand the conceptual network such as technologies (i.e. communication, hardware), policy aspects (i.e. organizational and personal policy adoption).

M. Babar, et al. have said that the composite approaches are completely entropy dependent, itis a qualification. Additionally, this hybrid approach made some use of soft computing opinions and lacked simulation information. Forecasting loads in the SG, different methods have been propounded, for example, Support-vector lag, intensive ML, enhanced secondary-array, error correction, and neural network. Large data analysis techniques for DSM have also been propounded [19].

I. Ahmed, et al. have proposed an approach dependent on a person monitoring algorithm based on ML features in an industrial environment. This executes a simple motion detection configuration through motion blobs and also in this calculation, rHOG Utilizes the history of the already filmed / bilobed population with the expected bubble position of the observer, comparing our results with five different tests sequences, with established mechanisms for object tracking. Additionally, this proposed tracking algorithm continuously monitors the static person for long periods by detecting, manipulating disturbances, manipulating abrupt change in the environment, and compensating for gaps in the data associated with all frames [20].

Bhattarai. P., et al. have presented a large data analysis on power grids and a comprehensive state review of its applications. It recognizing challenges and chances from the application, industry, and investigation viewpoint and analyzes research space, and provides insights into upcoming investigation directions to integrate large information analytics into energy system planning and functional structures. Complete data for applications seeking to use large information analytics and insights on how applications can improve revenue streams and giving troublesome innovations are explained. It also provides common guidelines for applications for making the correct investment in accepting large data analytics by revealing the interrelationships between critical infrastructure and functions [21].

Xingwang Li, et al. evaluated the wireless-powered decode-and-forward multilevel network's safety and reliability. In non-power gathering, IQI, and channel rating errors (CEEs) are taken into account. For best achievement, two relay choosing plans of actions are offered: 1) sub-optimal relay choice (SRS); 2) Optimal Relay selection (ORS). In particular, the correct analytical expressions for failure probability (OP) and interference probability (IP) are obtained in closed form. As for the IP, the signal from the eave's trapper source can be wired or a relay is considered. To gain increasing in-depth insights, then we execute the symptom analysis and diversity orders for OP in SNR (high signal-to-noise ratio) regimes.

Niklas Hossain., et al. have proposed a large information and ML application in the power phase developed by the upcoming generation power system-SG's aspects. At the heart of this framework connectivity's new phase, which is giving by IoT. This connection and constant contact needed in this method and also generated a large amount of information that required far superior methods when compared to usual methods of systematic investigation and decision making. The IoT-integrated SG network can give cost-effective well-organized load prediction and information acquisition technology. Large information analysis and ML methods are essential to reap these benefits. In SG's complex integrated system, CS becomes an important issue; internet of things (IoT) gadgets and their information will become the main targets of attacks [22].

3. The proposed safe requirement for the smart grid is the side management engine

The most significant element of the smart phase is the DSM, where consumers report applications on power consumption and respond to applications or manufacturers accordingly. Consumer needs to pass the real-time cost through electrical applications. Fig. 1 illustrated the planned safety status demand-side management (process) related to the SG and home area network (HAN). These home area networks (HAN) are integrated with SG, a subsidiary dedicated to DSM within the Smart Phase. These include demand response and energy proficiency, which is important elements in understanding the using the smart grid values

To monitor and manage the dedicated network home's power consumption, a home area network (HAN) is utilized. Manages its visitors and smart devices in the smart metering environment. The home area network has utilization that monitors the whole system. Smart phase, HAN, the home area of the market, and Smart Homes are now formed. There are more contacts with vendors SG-HAN because the applications seek ways to execute demand-side programs. The safe DSM machine in

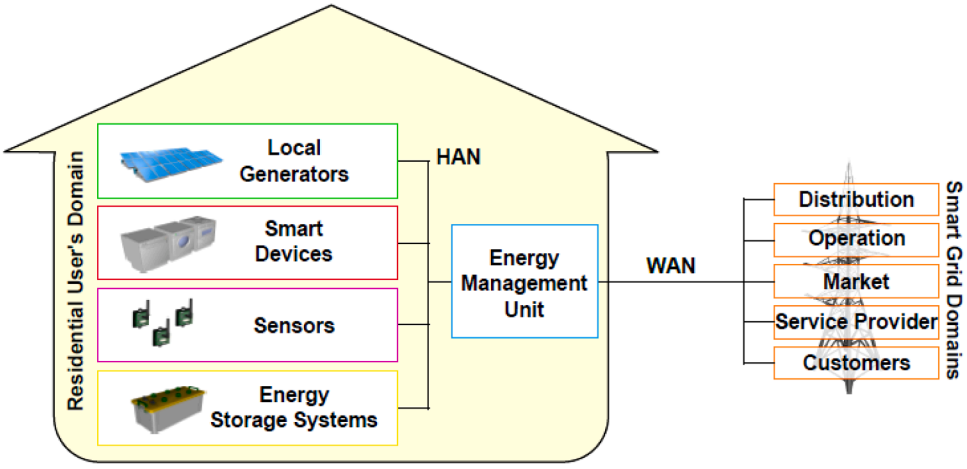

Fig. 1. DSM engine position.

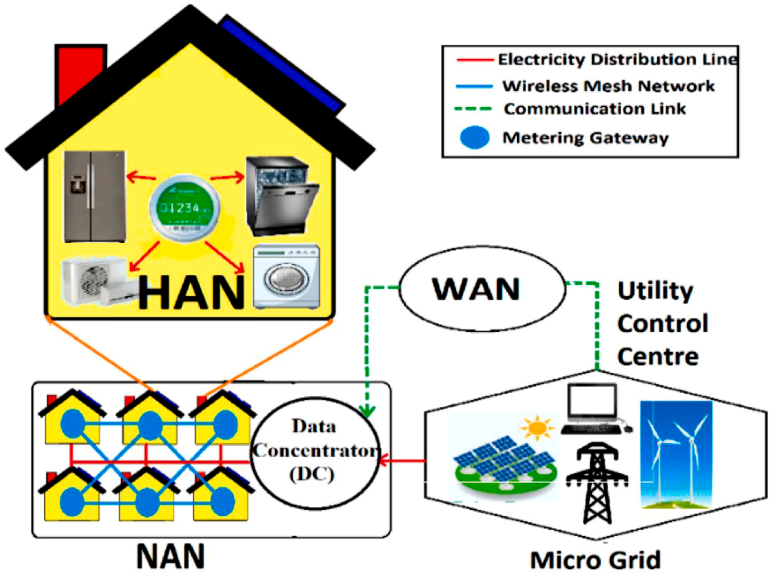

Fig. 2. System model.

the SG is utilized to maintain effective usage safely, depended on preferences and energy needs. High-power consuming and preferred devices are chosen and delivered promptly with approval within the parameters of specific constraints or load and cost limits. Figure-2 shows the propounded secure DSM engine's system model. There is no proposed model solution commercially available.

IoT-enabled Hans is the information source for the propounded safe demand-side management (DSM) machine [23]. The message recipient on the DSM machine receives this information, it is authorized to protect the message from Intrusive persons. In the smart grid, the protected data is processed to make decisions according to the needs and preferences of the consumers. The processing information outcomes are sent back to the home area network (HAN) for efficient resource usage. The outcomes can also be used for the technique called trend analysis for upcoming forecasting.

3.1. Resilient agent

There is a resilient agent in the planned structure to secure the grid from dangerous faults. In order to secure customer and vendor interactions, it operates within DSMs and built-in Hans and grid and offers regression by detecting dangerous units as compared to cyber assaults. RA's components are the Supplier Manager (PM), the Consumer Manager (CM), and the Control Analyst (MA). Managers who oversee the protection elements of the proposed resilient PM and CM-based agency [24]. The PM and PM treatment for caregivers and customers while AM is used to use the ML measure. In the proposed resilient address, the Naive Bayes (NB)- ML algorithm is used to identify correspondence as safe or unsafe. NB is indicated that as opposed to more strategies, the hypothesis of actual forecasters is right, it performs superior.

The PM is responsible for maintaining each provider's profile. This may have data for instance identity, skills, and level of trust, etc. The Chief is responsible for maintaining each consumer's profile. The functions of CM is depended on a quality variety. The resilient agent's monitoring analyzer in the proposed Demand Side Management (DSM) machine accepts communications without interruption. It separates forgery companies from contacting with the real person by categorizing various attacks.MA utilizing the NB machine learning method. However, classification and feature calibration are done before training.

The propounded resilience agent depended on NB calculation is utilized to predict the safety level deploying five various classes, which are good secure, fully secure, fairly secure, full insecure, partially insecure. Security score is calculated by using equation 1.

$$secLevel = \begin{cases} Full\,secure, & if\ S = 1 \\ Good\ secure, & if\ S \geq 0.76\ \ and\ S < 1 \\ Fairly\ secure, & if\ S \geq 0.51\ and\ S < 0.76 \\ Partially\ insecure, & if\ S \geq 0.26\ \ and\ S < 0.51 \\ Full\ insecure, & if\ S = 0\ and\ S < 0.26 \end{cases} \quad (1)$$

here, Eq. (2) is used to calculate S.

$$S = \frac{1}{n}\sum_{k=0}^{n} Fk \quad (2)$$

The F average for overall features is calculated later in its application.

3.2. Advance energy management agent

Additionally, to the Resilient Agent, the propounded DSM machine gives effective key functions power management. A particular unit AEMA is proposed to manage power efficiency use. The major aim of this AEMS element proposal is to meet consumer energy needs and conserve power efficiency. AEMS Contribution Journal Pre-Proof Achieving Efficient Resource Use especially improved power usage [25].

AEMA constitutes two major divisions

1. Electrical devices controlling system is helped by ZigBee sensor and
2.) Light sensor exploits natural illumination helps to light control system.

Power-user trusts heavily on the residential habitats functions within the home nature. Hence, the functions are implemented in a semi-automatic way, initialized by the client and AEMA control. The admin turns off a device by using the sends control command later than the client has run input. Operating time is an important parameter of system power consumption. When changing demands from the user, In the control station the time is saved. Because application control is dependent on client behavior, a user's event is periodically checked. If no user is detected during these specific checks, all devices powered by AEMA can be turned off to minimize energy wastage. At the same time, the management station update device switched off. Simultaneously to identify devices for control purposes individually, every electrical gadget is connected in the Zig-Bee sensor way [26]. Every sensor was allocated is a cognition number, which permits it to distinguish itself from another sensor in the smart home network. In unique, usage control should not interrupt with consumer fulfillment levels. In this way, an event dealing with the unit is embedded in the administration station to give a contact between the administration station and home clients.

Provides a control system to reduce the propounded AEMA power in the demand side management machine (DSM). The DSM control system adjusts the amount of light emitted by various smart devices on the home area (HAN) depended on the sunlight takeover area. The environmental parameter is defined and recognized in the four various scenarios according to the sunlight angle. DSM control method computes the needed light source luminosity in terms of the intensity received from the light sensor. The following relation is utilized to calculate the intensity () for the flight control system [27].

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

The control network is in charge of controlling the light intensity, taking into account environmental factors. A tuning factor has been generated for this intensity control. Eq. 4 is used to calculate intensity.

$$\varphi = \frac{FL_x \times L_M \times R_f}{\Gamma} \quad (4)$$

Here FL_x - whole luminous by a source,
LM - lumen,
Rf - lampshade echo constant, and
Γ - source length.

3.3. Interface control agent

ICA is evident from previous tests; synchronicity is corrupted by the complicated wireless hardware, the performance of each other. Due to synchronization, ICA prefers to enhance interface power. The proposed ICA does not accept this function. WLAN and ZigBee, IoT based WSN are used in the smart home network. Such methods operate on the 2.4 GHz ISM band, thereby contributing to disturbance of coexistence. Thus, we might assume that the difference between the nodes and the Wi-Fi connection point most influences the intrusion (AP). Another significant aspect to remember is that with the distance travelled to meet the target, the packet loss rate rises. Both these possibilities are often pointed to as harming the progress rate of data transmission, which in turn represents the efficiency deterioration of smart home appliances and gadgets.

ZigBee coordinators are then formed in this system. The leadership of the coordinator is to reduce the result of packet failure from interference with co-existence and the gap between the management station and sensor nodes. Any space in the house and kitchen is equipped with a ZigBee coordinator. As physical space is an essential consideration for intrusion, limited interference within the same community is guaranteed by the required position of the ZigBee coordinator. It therefore decreases the number of hops between the source and the target, effectively reducing the loss of packets.

Both sensor nodes in the smart home are grouped into n categories in view of the gap between the sensor and the Wi-Fi AP. As the current project assumes the coexistence of Zig-Bee WSN and WLAN interruptions, the positioning of communicating WIFI AP and sensors has been considered. Sensors belonging to category 1 in the vicinity (G1). A remote threshold (d [σ1]) corresponds to the sensor in G1. The gap here is smaller than the threshold - d<d[σ1]. Likewise, the remaining sensor nodes are correspondingly clustered into G2…Gn following the raised distance threshold d[σ2] <d[σ3].....d[σn]. As proximity to Wi-Fi results, the sensors in the G1 suffered from the highest rate of interference. When a Zig-Bee channel is taken over by WLAN links, it typically raises the tendency of WLAN signals to take over nearby channels. To cope with the consequences of the above case, we therefore assign one channel to each category G. For sensors in G1, non-interconnected channels are allocated since they are the nearest sensors to the Wi-Fi AP. The channel from G2 to Gn is assigned depending on the findings obtained according to the MADM model. The MADM approach fulfills a criterion (c) in this case, which requires bandwidth, efficiency, and violence.

The work on the MADM-based channel is listed below.

I Classification and normalization of the steps into a network of decisions
II Building the weighted judgement matrix
III For the good supreme ideal and the bad ideal state, measure
IV Calculate the division between supreme circumstances, favorable and negative,
V Measure the channel ranks accessible Every measurement, the weight (w) is allocated as $wx = cx/\sum cx\,y\,x = 2$.As a result of the ranking calculation, in ascending order the channels are

arranged. Closer grouping to WIFI AP which allocated to drains with more teams. In the end, a seamless home network ensures seamless communications ICS, which is equipped with multiple wireless techniques.

3.4. Parameters, methods, and trade-offs DSM machine's

After the data and messages authorization, DSM is in charge of maintaining effective power use depended on energy priorities and demands. Power efficiency usage is done based on the selection of techniques based on the parameters, demand, and preferences that affect the performance of the smart grid and the trade exchange of the consumer. In Tabulation 1 a performance parameters list or restriction for the SG is narrated.

The DSM's final parameter is the gadget's priorities. In Tabulation 2 these are narrated. Which are attacking the DSM methods and inverse. These affecting parameters are heavily related to a greater trade-off conclusion.

The techniques illustrated in Fig. 3 are utilized to attain the demand-side management (DSM) machine aim's to remain consistent in amount and load limits. The provider's view of the primary form of primary concern's load is about secondary concern from a consumer perspective. D.S. These techniques of Marine are also described in Tabulation 3.

4. Result & discussion

In this section, a detailed study and discussion of the outcome attained by deploying the proposed modules are discussed. The proposed reversible DSM machine's performance is especially expressed by the pre-simulated system.

Two sets of tests were performed they are

1 Resilient machine tests utilizing Naïve Bayes algorithms including model training. Specific reliable and accurate databases are utilized to teach the model to differentiate between secure and insecure contact entities or things.
2 Evaluation of the overall DSM machine's power efficiency for a particular HAN different display with standard WIFI APs deploying C # high-level programming. On genuine databases, stream processing is also executed.

Re-evaluation is executed by an engineering agent for a particular environment. Initially, the propounded flexibility agent was trained using an assortment in the (340 × 900) matrix, which is an estimate of 900 services with 340 consumers. NB algorithms make the premise that in a class of one feature is nota part of another. In Fig. 4 the NB classifier's training was illustrated.

Computing the resilient agent, the proposed classifier's efficiency, a confusing matrix is used as shown in Tabulation 5. Precision is assessed in the condition of both accurate and insecure classes. The confusing matrix is preferred because it gives the best view of the classification model. Additionally, it is the most broadly utilized performance measurement method for ML Algorithms.

If the value of S is greater than or equal to 0.51 then less than 0.5 is considered safe. Considering these terms because it was taken into an account in the previous terms. In tabulation 6 the results of the propounded sample are shown. The details of the confusing matrix rules are as follows:

- If TP is a value set classified as safe contact by the propounded resilient agent, which is 94% deploying the propounded sample.
- If TN is a value set classified as safe contacts secure by the proposed flexibility address of 6% deploying the propounded model.
- If FP proposed for safe contact, secure, resilient agent classified as a set of values, which is 7% deploying the propounded model.
- If TN-secure communication between the agent proposed a resilient set of values differentiated by the secure, using the proposed model is 93%

The energy potential of the proposed architecture is evaluated for various scenarios. To compute the DSM performance, C # high-level programming language is utilized. A particular HAN with standard WIFI Aps is designed. Due to the permit of Hans to connect grid applications intelligently, HAN simulations are preferred. This is because of the HAN-centric access to multiple gadgets and appliances. Additionally, this has mechanism effectiveness for power saving.

The two functions are performed by the client that are turned-off approximately and run on an Internet of Things (IoT) device for five hrs. and generate continuous traffic with a certain power series (1001 to 5001 bytes). IoT sensor's Power consumption and gadgets are computed by considering the customer activity as Random variables, i.e. 6 to 35 s. Practically, the simulation period is changed to 5 to 15 min per burner. Moreover, 1799 lm, 70%, 2.21, and 329 mm with LM, RF, FL, and 0 in various chambers. The room size is 3100 mm. When the user stays in a particular room for 6–12 min, it is automatically turned off and on the IoT in the room.

The power utilization of IoT-enabled smart devices for instance AB-1, AB-2, AB3, and AB-4, in Fig. 5 (a) to Fig. 5 (d) shows the estimation by

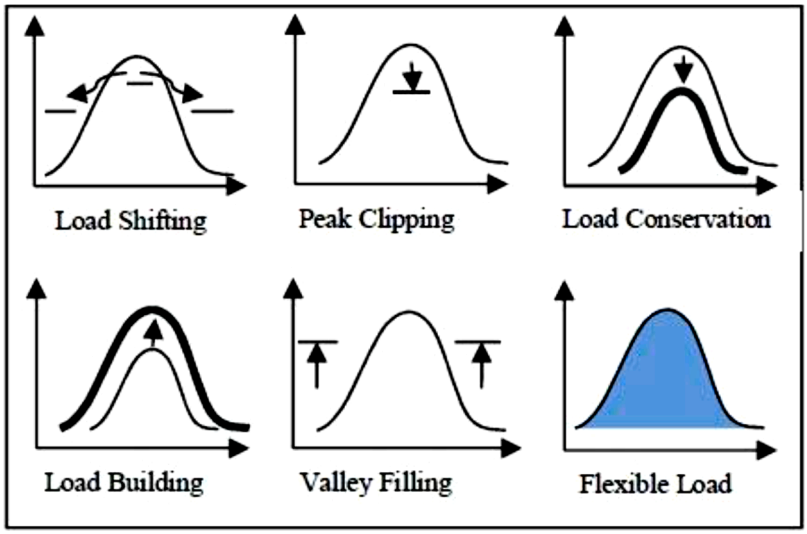

Fig 3. DSM Techniques.

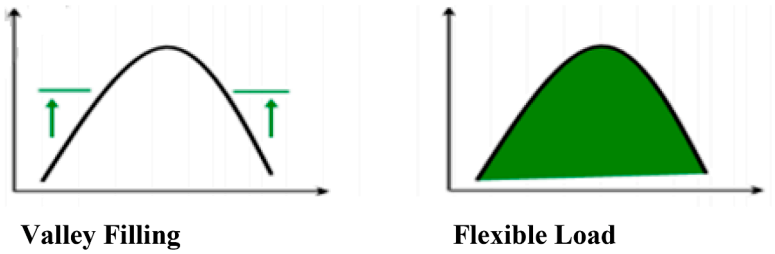

Fig 4. Model training.

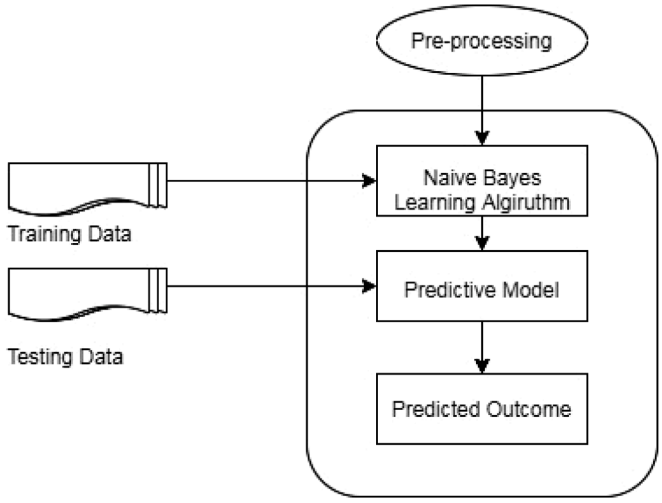

Fig 5. Proposed DSM engine's energy efficiency.

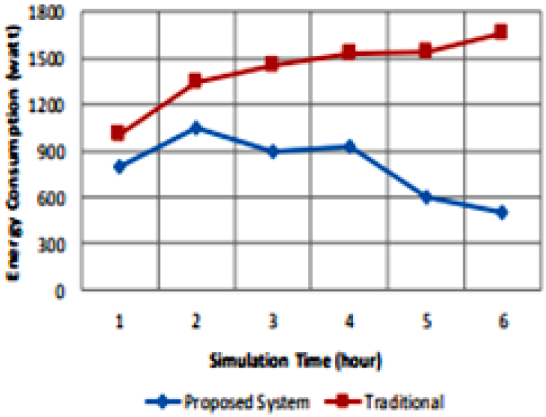

Fig 6. Other node's power utilization.

using the proposed and conventional schemes. Accordingly Utilizing the DSM engine significantly reduces the power consumption of smart devices. Besides, the application manages and monitors the energy consumption usage of the smart device by research histories. The important parameters to be considered are the user's priority and need. The proposed DSM machines integrated with HAN drive devices on and off based on client needs and first rights for saving inappropriate energy usage.

Furthermore, trends can be analyzed using information recorded in the DSM. Subsequently, a client can take advantage of the power of devices. Similarly, Fig. 6 shows the room light source's power consumption. The power consumption is decreased by utilizing the propounded approach because of an Advanced Energy Management managing energy-efficiency use. Furthermore, the power requirements of different nodes at various times.

5. Conclusion

Integrating communication technologies and sensors into power structures approved as an SG. In these stressful problems, safety is the most serious one, which is the greatest challenge to the SG. In this paper, the safe and flexible DSM machine using machine learning is recommended to protect the internet of things-IoT-enabled from crucial offensives. DSMs are liable for maintaining energy efficiency use depended on greater importance and requirements. A particular resilient agent model is propounded and also a particular flexibility agent model has been proposed to control incursions and the SG demand-side management (DSM). Resilient agent predicts fraudulent companies by utilizing the machine learning classifiers. A processing module has been propounded in the demand side management engine to process power data produced by the Internet of Things (IoT)-enabled home area network (HAN) to improve power use. An implemented efficiency of Simulation is also to experiment with the proposed project's effectiveness. A particular home area network (HAN) is structured with standard Wi-Fi. The outcome of the analysis shows that the planned demand-side management (DSM) machine is lower susceptible to the incursion and may be sufficient to decrease the energy consumption of the DSM on the SG and associated home area network (HAN) gadgets.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

References

[1] FakhriiAlam Khan, et al., Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development, Sustain. Cities Soc. (2020), 102018.
[2] Panagiotis I. Radoglou-Grammatikis, Panagiotis G. Sarigiannidis, Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems, IEEE Access 7 (2019) 46595–46620. Jo.
[3] Tanveer Ahmad, Hongcai Zhang, Biao Yan, A review on renewable energy and electricity requirement forecasting models for smart grid and buildings, Sustain. Cities Soc. (2020), 102052.
[4] Tejasvi Alladi, et al., Blockchain in smart grids: a review on different use cases, Sensors 19.22 (2019) 4862.
[5] Prosanta Gope, Biplab Sikdar, Privacy-aware authenticated key agreement scheme for secure smart grid communication, IEEE Trans. Smart Grid 10.4 (2018) 3953–3962.
[6] Mohammed Ali Al-Garage, et al., A survey of the machine and deep learning methods for the internet of things (IoT) security, IEEE Commun. Surveys Tuts. (2020).
[7] Jiyoung Lim, Inshil Doh, Kijoon Chae, Secure and structured IoT smart grid system management, Int. J. Web Grid Serv. 13.2 (2017) 170–185.
[8] Federico Passerini, Andrea M. Tonello, Smart grid monitoring using power line modems: anomaly detection and localization, IEEE Trans. Smart Grid 10.6 (2019) 6178–6186.
[9] Sean Weerakkody, Bruno Sinopoli, Challenges and opportunities: cyber-physical security in the smart grid, Smart Grid Control (2019) 257–273.
[10] Mohammad Abujubbeh, Fadi Al-Tudjman, Murat Fahrioglu, Software-defined wireless sensor networks in smart grids: an overview, Sustain. Cities Soc. (2019), 101754.

[11] Sadia Din, et al., Constrained application for mobility management using embedded devices in the Internet of Things based urban planning in smart cities, Sustain. Cities Soc. 44 (2019) 144–151.
[12] Fadi Al-Tudjman, Mohammad Abujubbeh, IoT-enabled smart grid via SM: an overview, Future Gener. Comput. Syst. 96 (2019) 579–590.
[13] Malik Qasaimeh, Rawan Turab, Raad S. Al-Qantas, Authentication techniques in smart grid: a systematic review, Telkomnika 17 (2019) 1584–1594.
[14] Sandeep Nair Narayanan, et al., Security in smart cyber-physical systems: a case study on smart grids and smart cars. Smart Cities Cybersecurity and Privacy, Elsevier, 2019, pp. 147–163.
[15] Pradeep K. Khatua, et al., Application and assessment of internet of things toward the sustainability of energy systems: Challenges and issues, Sustain. Cities Soc. 53 (2020), 101957.
[16] M. Babar, F. Arif, M.A. Jan, Z. Tan, F. Khan, Urban data management system: towards big data analytics for Internet of Things based smart urban environment using customized Hadoop, Future Gener. Comput. Syst. 96 (2019) 398–409.
[17] Fernando Lezama, et al., Flexibility management model of home appliances to support DSO requests in smart grids, Sustain. Cities Soc. 55 (2020), 102048.
[18] Dharmendra Yadav, Anjali R. Mahajan, A. Thomas, Security risk analysis approach for a smart grid, Int. J. Smart Grid Green Commun. 1.3 (2018) 206–215.
[19] Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, Ekram Hossain, Machine learning in IoT security: current solutions and future challenges, IEEE Commun. Surveys Tuts. (2020).
[20] Tolga Toyota, et al., Smart cities in crisis: technology and policy concerns", Sustain. Cities Soc. 50 (2019), 101566.
[21] M. Babar, F. Arif, Real-time data processing scheme using big data analytics in the internet of things based smart transportation environment, J. Ambient Intell. Humaniz Comput. (2018) 1–11.
[22] I. Ahmed, A. Ahmad, F. Piccialli, A.K. Sangaiah, G. Jeon, A robust features-based person tracker for overhead views in an industrial environment, IEEE Internet Things J. 5 (3) (2018) 1598–1605.
[23] B.P. Bhattarai, S. Paudyal, Y. Luo, M. Mohanpurkar, K. Cheung, R. Tonkoski, M. Manic, Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions, IET Smart Grid 2 (2) (2019) 141–154.
[24] Xingwang Li, Mengyan Huang, Yuanwei Liu, Varun G Menon, Anand Paul, Zhiguo Ding, I/Q Imbalance Aware Nonlinear Wireless-Powered Relaying of B5G Networks: Security and Reliability Analysis, 2020 arXiv preprint arXiv: 2006.03902.
[25] Niklas Hossain, Imtiaz khan, Fuad Un-Noor, Sarder Shazali Sikander, Samiul Haque Sunny, Application of big data and machine learning in smart grid, and associated security concerns: a review, Application of Big Data and Machine Learning in SG, and Associated Security Concerns 7 (2019) 2169–3536.
[26] Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli, Cyber-physical systems security: limitations, issues and future trends, Microprocess. Microsyst. 77 (2020), 103201. ISSN 0141-9331https://doi.org/10.1016/j.micpro.2020.103201, http://www.sciencedirect.com/science/article/pii/S0141933120303689.
[27] Hao Piao, Hanming Duan, Miaomiao Zhu, Simulation of urban landscape around subway station based on machine learning and virtual reality, Microprocess. Microsyst. (2020), 103495. ISSN 0141-9331https://doi.org/10.1016/j.micpro.2020.103495, http://www.sciencedirect.com/science/article/pii/S0141933120306475.

Shweta Chandrashekhar Dharmadhikari received the B.E. in CSE from NMU, Jalgaon, Maharashtra, in 2002, M.E. in CSE from BVDU, Pune, Maharashtra, India, in 2005 and the Ph.D. in Computer Science from Devi Ahilya Vishwa Vidyalaya, Indore (M.P.), India. She has been in teaching profession for more than 18 years. She has attended many conferences, workshops, short-term courses, conducted seminars, workshops and delivered guest lectures. She has guided many UG and PG projects. She is presently working as Associate Professor in Department of Information Technology at Pune Institute of Computer Technology, Pune.

She has 7 IPRs to her credit out of which two are Granted International Patents, two Published Indian Patents and three registered Copyrights. She has over 35+ research papers published in various International/ National Journals and Conferences.

Dr. Veerraju Gampala, earned his doctorate from Acharya Nagarjuna University, Guntur, Master Degree in Computer Science and Engineering from JNTU University, Kakinada, Bachelor Degree, from JNTU University, Hyderabad. He is currently working as an Associate Professor in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KL University), Guntur, Andhra Pradesh. He has more than 14 years of Teaching and 6 years of Research experience. He has 25 research publications in reputed journals which are indexed by Web of Science and SCOPUS also. He guided 14 UG projects and 4 PG projects. He has organized one National workshop. He is currently guiding one PhD scholar.

He has received "Best Teacher Award" in 2012, 2013, and 2014 from GMR Institute of Technology. He has completed global certifications such Robotic Process Automation, Angular, Node.js, Rest API etc. He has completed more than 50 online certification courses from reputed universities and organizations like Coursera, edx, saylor etc. Apart from research, administration he has implemented OBE based teaching in class-room, flipped learning etc. His-research interests are Cryptography, Cloud Computing, Artificial Intelligence, IoT, and Bigdata Analytics.

Dr. Ch. Mallikarjuna Rao received the B. Tech degree in Computer Science and Engineering from Dr. Baba Sahib Ambedkar Marathwada University, Aurangabad, Maharastra in 1998, M. Tech Degree in Computer Science and Engineering from JNTU Ananthapuramu, Andhrapradesh in 2007 and Ph.D in Computer Science and Engineering from JNTU, Ananthapuramu, Andhrapradesh in 2016 Currently he is working in " Gokaraju Rangaraju Institute of Engineering and Technology", Hyderabad. Telangana, India. His-area of Interests are Data Mining, Bigdata and Software Engineering

Dr. Syed Khasim, Obtained Ph.D degree in Computer Science & Engineering from Rayalaseema University, Kurnool, Andhra Pradesh, India. At present, working as a Professor in Department of Computer Science & Engineering in Dr.Samuel George Institute of Engineering & Technology, Markapur, Andhra Pradesh, India. Having 16 years of experience in Teaching and Research. Published Various National and International Journals. His-research interests include Software Engineering, algorithm design and analysis, Internet of things, Machine learning & AI.

Dr. SHAFALI JAIN received the B.E. (Hons.) degree in Electrical Engineering from Samrat Ashok Technological Institute, Vidisha (M.P), India in 2003, M.E. (Hons.) degree in Electrical Machines and Drives from Samrat Ashok Technological Institute, Vidisha (M.P), India in 2006 and PhD degree in Electrical Engineering from Maulana Azad National Institute of Technology, Bhopal (M.P)-India in 2012. She currently holds a position of Head of department of Electrical and Electronics Engg, Sagar Institute of Research and Technology, Bhopal (M.P)-India.

Her research interests include are power system restructuring, power system operation and management, Energy and Electric Vehicles. Dr. Shafali Jain was a recipient of Silver medalist (Second university topper) in M.E. in 2006.

R. Bhaskaran received his B.E., Degree in Electronics & Communication Engineering from Madurai Kamaraj University in 2002 and M.E., Degree in Computer Science & Engineering from Anna University and the Ph.D., Degree from Anna University, Chennai. He currently holds the position of Professor in the Department of Information Technology, PSNA College of Engineering and Technology,Dindigul, Tamilnadu. India. His-area of work includes ADHOC Grid, Job Scheduling, Under Water Sensor Networks, Machine Learning & Internet of Things. He has 17 years of teaching experience in the department of information technology. He has published 12 research papers and 20 papers national and international conferences. He is also a member of ISTE, AC