Journal of Electronics and Informatics (2021)
Vol.03/ No.01
Pages: 1-14
https://www.irojournals.com/iroei/
DOI: https://doi.org/10.36548/jei.2021.1.001

Smart Home Environment Future Challenges and Issues - A Survey

Sathesh,
Department of EEE,
Eritrea Institute of Technology,
Eritrea.
Email: sathesh4you@gmail.com

Yasir Babiker Hamdan,
International University of Africa (IUA),
Khartoum,
Sudan.
Email: yasir20ap@iua.edu.sd

Abstract- The smart home automation is that the exploitation internet enabled devices remotely and mechanically management appliances such as lighting, heating system and security measures in and around your home. This papers talks about relative emission effects in Home Energy Management. Also the result outcome is that consumption of the electricity will be reduced towards green environment. Moreover, the research paper is considering the analysis of calculate the negative effects in environment due to full home automation system. While calculating these negative effects, the Life Cycle Assessment (LCA) should be in sum total. This study uses to analysis the electricity consumption for environment impact of Home Energy Management system (HEMs). The research article discusses home automation system consumes the energy for different devices connected for smart home. The maximum energy consumption in smart home network is smart plugs due to an uninterrupted supply. Therefore this research article comprises about home automation energy management that shows the balance energy consumption between the devices in a regular interval. Also this research article provides a future challenge tasks in security issues in smart home environment. Also the perception for smart home environment focuses the Interoperability, Reliability, Integration of smart homes and term privacy in context, term security and privacy vulnerabilities to smart home.

Keywords: *HEMS, IoT*

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

1. INTRODUCTION

Every human wants to be a comfort life style with safety manner. In many developed and full time cold countries, they may use their phone to show on the kitchen appliance even as you are feat work so dinner is prepared by the time they arrive home [1]. Otherwise synchronize the heating with weather forecast to create positive their home is never unduly cold.

The smart home can be named in many terms as follows; “Home Automation”, “Assistive technology”, “e-health”, “digital in house”, “smart environment”, “automated house”, “smart connected home” & “intelligent in living”. Also our life style is moving towards comfort in living environment gradually [2]. The development of the IoT is mixed with many factors and smart sensors. The data is exchanging between the various sensors and home automation system to user mobile devices [3, 4]. The figure 1 shows simple IoT devices for smart home environment.

Figure 1 The Smart Home Environment

The smart home should be contained with many machine driven sensors and customized systems for secure life elegance. The security issues are having different types and which increases day by day in our regular life [5]. However, the attacks exist with many associations of techniques and interrupt in the smart home management system. There are primarily 2 kinds of threats as follows;

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

1. Information privacy

2. Context aware privacy

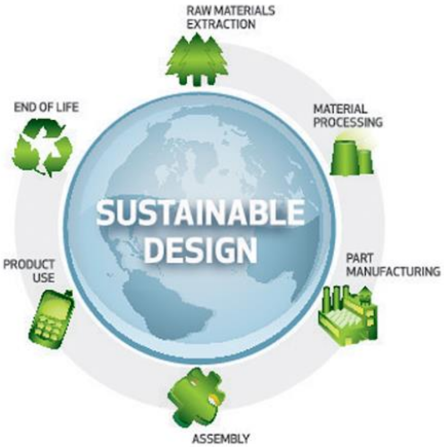


Figure 2 Life Cycle Assessment

The figure 2 shows the LCA for sustainable design. Information privacy is a vital concern once it involves exchanging valuable info concerning something. The hackers are penetrating in the network which is connected and associated with sensors and smart home system in a simple manner unless strong firewall protection. The recognizing, identifying category is comes under context attentive and privacy [6]. The identifying factors are modifying to intellect and answer back towards energy consumption. Privacy may be a generic term which means of that change with values, interval and age band [7, 8]. The overview of HEMS is shown in figure 3.

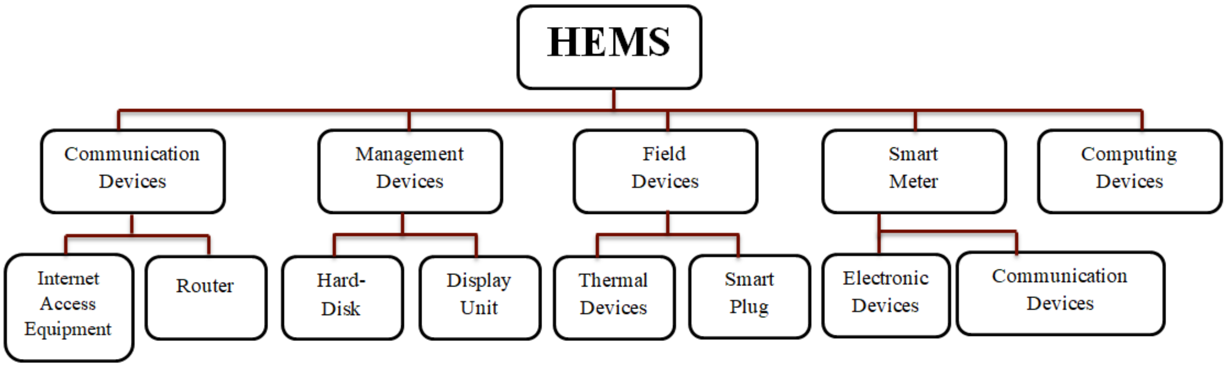


Figure 3 Overview of Home Energy Management System

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

The figure 3 shows many devices category and it comes under management system. The smart home needs further in not disturbed by any person named as privacy [9]. Also the personal information of the user will be more protected principally [10]. The smart mobile devices are storing our personal details and operated from remotely which needs privacy and authentication. New devices (Amazon Alexa and Google Home) might hear non-public conversations after listened from voice commands. Here this information should be safeguarded for the future [11]. The important factors of smart home environment are smart economy, movement, atmosphere parameters, authority control as shown in figure 4 in detail.

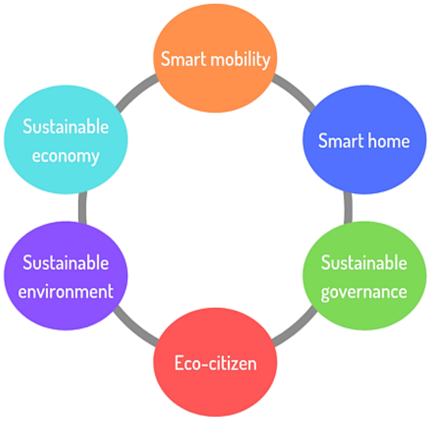


Figure 4 Factors for smart home environment

2. ORGANIZATION OF THE RESEARCH

The structure of the research article organized as follows; Section 3 provides preliminaries, of recent security based IoT and its privacy importance. Section 4 provides the description of methodologies. Section 5 delivers description of results and discussion finally the conclusion and future enhancement is in section 6.

3. RELATED WORKS

Atzori et al present the various range application in IoT [12]. Xu et al reviews the smart home environment issues such as reliability, redundancy, security and suitability [13]. Joy Iong Zong Chen and et al highlighted current scenario of solving IoT authentication issues with the help

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

of hybrid Deep Learning (DL) techniques with Reinforcement Learning (RL). Also they compared previous DL methods with accuracy metric measurement [14].

Ahmed Atamli et al propose the frame work and supporting tools for interfacing between user agents and sensors which exist in home. Also it provides practical model for risk valuation model. This work focuses attack minimization and gives good control in security to the user agent that is house owner [9]. Drushti Desail et al addressed the safety and privacy issues for home environment. The parameter associated with knowledge minded privacy and context minded privacy are measured. This paper discusses the concerning safety and privacy problems in home automation system. The cryptologic procedures are one of the great gifts for home environment. The author have steered new legal thought that must be targeted and have planned new protocol for minimizing the privacy problems [15].

Huichen Lin et al discusses about key problems in energy saving for home automation system. Also they propose the impact of access design for IoT applications. The configuration design and modernizes in programmed version is dealt in this research paper. And they have done the framework for this configuration security features for smart home environment [10].

H. Manoj et al has written about security and authentication problems during access of smart home automation. They are trying to judge the effects and causes during authentication and access control. Also they gave legal, robust communication outline to the smart home environment [16].

The internet range is in smart home range connected that some huge area. Even though the problems exist in privacy and authentication the home becomes smarter. Many research paper suggests the outlined about network sentiment analysis for the higher security protection. The security in home automation by the users is provided for improving the protection level there by Internet Service Provider (ISP). However victimization sentimental analysis users will amendment it [17]. C.Ramakrishna et al proposes some solution for attacks in IoT for smart home environment. Also they look forward about wireless network attack and recent techniques [18]. Yuchen Yang et al are addressing the protection and confidential problems in IoT networks. Also they well planned and organized construction for security problems in IoT networks [19]. Eric Zeng et al investigate security problems within the sensible home atmosphere victimization for safety in IoT networks. Also their approach is very useful for future IoT network investigators and researchers [20]. Marlen S Bissaliyev et al introduces the protection concern in standard version for IoT network devices. The physical attacks has discussed and provided a smart solution to safest IoT devices [21].

Ali Dorri et al investigate block chain technology for IoT appliances for smart home environment system. They have configured some more solutions for network traffic, execution time and electricity consumption in smart home [22]. Joseph Bugeja provides some challenging task for home automation systems. They targeted some sensor and statement problem [23]. They recognized four vital challenges that want to concentrate additional attention for the following uniqueness supervision, checking of hazard, the exchange of data, authentication supervision methods. Sathish et al focuses the life style enhancement based improvement in home automation environment such as energy saves and energy consumption which will make pleasant surrounding [24].

RESEARCH GAP

The service devices will interact with the help of network devices which interconnect all service devices. Sometime due to network congestion or fails, there will be a massive loss in beneficial side. Also during this time there is no guarantee of security and safety concern. Above said all research paper poor in maintain the environmental status and LCA around any smart home.

The observe of smart home automation or the interconnectivity of domestic appliances, lighting, heating and security measures through the internet is turning into a lot of and lot of common within any country and abroad. One among the reputed merchandising points of such a system is that the helpful effects it’s on the atmosphere by optimizing the employment of energy

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

and flattening peak consumption rate. While previous studies have seemed to support such a hypothesis, a brand new paper from many European nations suggests this could not be the case. The finding solid aspersions on the effectiveness for good home automation are having more number of a viable environmental tool. Generally, there must be improvements in

1. Security – Cameras & Alarms in many domestic appliances
2. Access control - Device authentication
3. Firewalls and Intrusion prevention system - Network access policy
4. Updates and patches – Attacks through internets
5. Environmental – Water meter, Energy management lighting, temperature, humidity sensor

4. METHODOLOGIES

The smart home environment offers to appropriate home setup where domestic appliances and devices connected together through internet which controlled by any mobile or remote device from anywhere. According to the house owner's desire, the facility of every smart home can be setup with help of service devices [11, 25].

The smart meter is taken into account to be a permanent half during this proposed system. We tend to thought about associate degree existing smart meter. We tend to restrict with the number of knowledge on the market, particularly in terms of parts gift and their quantities. As no information regarding the accurate conditions of every component that are set within the system, certain expectations are created.

4.1 Energy management

The smart meter is one of the equipment that registers a digital signal with Central Process Unit (CPU). The communication devices will be shaped and records by smart meter. During this case, it's thought about that the communication among the building and goes to the surface need additional instrumentality.

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

4.2 Integration of Smart homes

In essence of smart home were primarily conceptualized and later developed to mechanically address the daily necessities of aged and users with disabilities. Likewise, with this international agendas for achieving property urban future, smart homes became a lot of and a lot of tangled with advanced property technologies. A lot of recently, alternative users have additionally shown interest to measure in such extremely machine driven homes. Nonetheless, it is often argued that there’s an important for the smart home to confirm harmoniousness between the planning of living close, style of occupants and also the senses of embedded intelligent technologies. Likewise, smart homes ought to be able to unceasingly adapt themselves to the speedy changes of technology and occupant’s desires.

4.3 Reliability

In associate integrated smart home, completely different appliances / devices are interconnected with variable tolerances for technical errors. This variation of tolerance raises serious issues as example boiler designers and residential PC developers could have completely different assumptions concerning the suitable level of tolerance for crashes. Likewise, even insignificant malfunctions within the computing machine may probably cause dangerous malfunctions within the boiler.

4.4 Energy Control Technique

It is suggested that the potency of smart homes is anticipated to be climaxed whereas utilizing real-time approaches. The simulation results disclosed that the projected system will decrease the peak to average quantitative relation of the full energy demand, the full energy value in addition as user’s individual daily electricity charge.

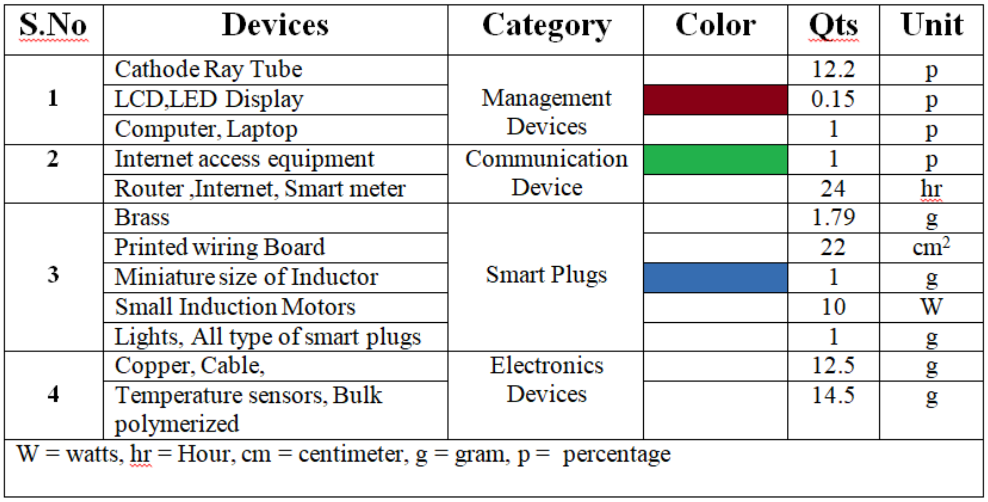
Energy management in smart homes is regarding making an attempt to extend the management over the manage energy consumption. Many researchers have used embedded PC intelligence in order to optimize the facility consumption of governable appliances. This was done based mostly on retail evaluation schemes, information regarding numerous home appliances and call trees based mostly on their consumption behavior. This platform provided for us also a straight forward access to choose displays of switching standing and consumption of all appliances. Remote summary of the data and power use management via smart phone and terminal computer was conjointly authorized.

5. RESULTS DISCUSSION

The table 1 shows different devices in a category with its usages. The relative emission impact for each category devices shows in the graph figure 6. In the graph, WD – Water Depletion, IR – Ionizing Radiation, FE – Freshwater Eco toxicity, OF – photochemical Oxidant Formation, HT – Human Toxicity, OD – Ozone Depletion, CC – Climate Change. In WD, the smart plug is having more relative emission. In HT, smart plug is having less relative emission related with other management devices.

Smart plugs will scan the electricity consumption of associate degree appliance. The smart home environment system contains own precise load for all sensor modules. There smart plug contains natural pins, casting with natural plastics insider of plugs. This device is used to obtain the data from various sensor modules and calculating for the home automation system. The energy saving is mainly focuses in management system due to huge consumption of energy in their module.

Table 1 Smart devices used in smart home



S.No	Devices	Category	Color	Qts	Unit
1	Cathode Ray Tube	Management Devices		12.2	p
	LCD,LED Display		🟥	0.15	p
	Computer, Laptop			1	p
2	Internet access equipment	Communication Device	🟩	1	p
	Router ,Internet, Smart meter			24	hr
3	Brass	Smart Plugs		1.79	g
	Printed wiring Board			22	cm^2
	Miniature size of Inductor		🟦	1	g
	Small Induction Motors			10	W
	Lights, All type of smart plugs			1	g
4	Copper, Cable,	Electronics Devices		12.5	g
	Temperature sensors, Bulk polymerized			14.5	g

W = watts, hr = Hour, cm = centimeter, g = gram, p = percentage

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

The field devices in home automated system, many sensing element is connected with smart plug. This smart plug is recording the reading of many field devices reading and configuring in the home automation system.

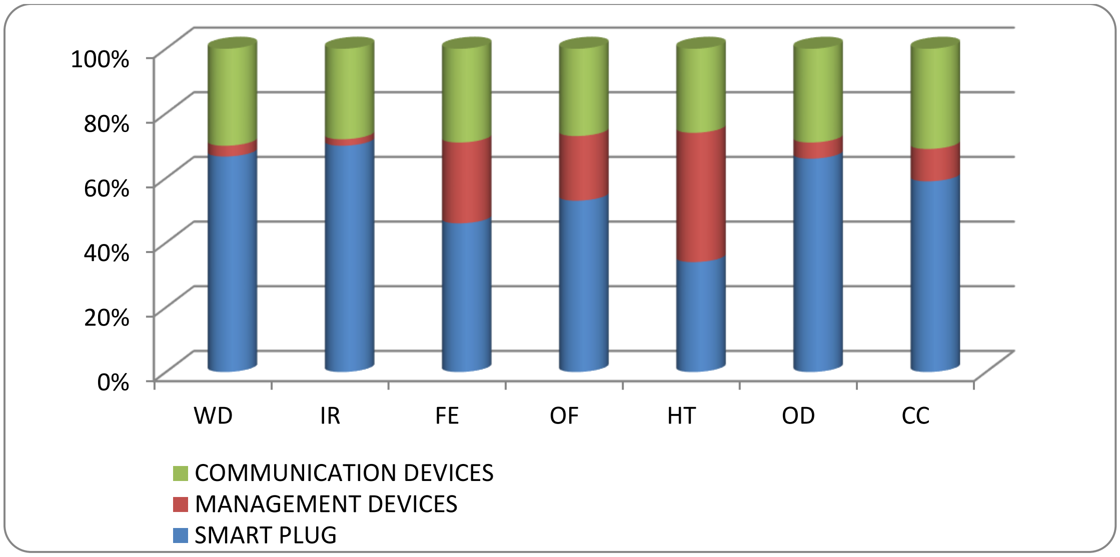


Figure 6 Relative emissions impact for each component in smart home environment

The smart plug contains more relative emission characteristic in all factors as shown in the graph. But the human toxicity concentrates of more number of desktop, laptop. Therefore there must be a minimal of field devices causes. Also it will control by remotely as well as directly with in the environment setup around the home automation. Also this result discussion will be shown for differentiating between the devices usage. Accordingly, the energy consumption can be reduced by controlling various devices in home automation environment.

6. CONCLUSION

Our suggesting methodologies can minimize the energy consumption in various home appliances and it provides the overall good electricity consumption. The around 18 equipment electricity consumption will be our consideration in home automated system. This energy should be controlled and managed for the smart home fully automated system for green environment.

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

Also the LCA study in this paper provides good impact in energy saving configuration. This research work focuses energy consumption in two different environments. First one is normal without any control and managing of various devices with overall calculation. Here we got a result in energy consumption for overall model is 3511.12kWh.

Next one is the energy is controlled and managed by our suggesting methodologies and got the energy consumption is 3255.17kWh. Therefore overall energy consumption difference is 255.95kWh in smart home automation network system. While Indian regulation focuses on phase of sensorial devices and green environment. This environment effect is providing this good energy saving per unit and it leads to smart home atmosphere quickly. Also our survey is about the relative emission impact of each and every component which is associated with IoT smart network system. One in all the weak points of the conferred LCA assessment is that it considers a hard and fast emission issue. We are able to conclude that we had to like to seek out the balance between what we have a tendency to really want to manage between LCA assessment and energy consumption.

Future challenges in Smart Home Environment

The optimum energy consumption is a big challenge for smart home in still and future too. The interoperability allows information associated properties is modified between the various sensorial module in smart home environment’s row. Still there is a challenge task is that the absence of proper row communication between the connected devices which is in smart home environment. During the consistent operation of various integrated devices, there may be delay assimilation interruption with any new devices. These problems have to sort out in our proposed methodologies in smart homes works under artificial networks in the IoT smart home network. Within green environment of fully automated smart homes, the ability is often outlined “the state of communication completely different devices with one another into a same network context”. Nonetheless, achieving this will be extremely complicated because the connected sensorial devices comprehend completely various networks for smart home environment system.

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021

REFERENCES

[1] Ghaffarianhoseini, Ali & Tookey, John & Omrany, Hossein & Fleury, Anthony & Naismith, Nicola & Ghaffarianhoseini, Mahdiar. (2016). The essence of smart homes: Application of intelligent technologies towards smarter urban future. 10.4018/978-1-5225-1759-7.ch004.

[2] Louis, Jean-Nicolas & Caló, Antonio & Leiviskä, Kauko & Pongrácz, Eva. (2015). Environmental Impacts and Benefits of Smart Home Automation: Life Cycle Assessment of Home Energy Management System. IFAC-PapersOnLine. 48. 10.1016/j.ifacol.2015.05.158.

[3] Miraz, Dr & Ali, Maaruf & Excell, Peter & Picking, Rich. (2018). Internet of Nano-Things, Things and Everything: Future Growth Trends. Future Internet. 10. 10.3390/fi10080068.

[4] Lin, Huichen & Bergmann, Neil. (2016). IoT Privacy and Security Challenges for Smart Home Environments. Information. 7. 44. 10.3390/info7030044.

[5] J. Bugeja, A. Jacobsson and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," *2016 European Intelligence and Security Informatics Conference (EISIC)*, Uppsala, 2016, pp. 172-175, doi: 10.1109/EISIC.2016.044.

[6] Jurcut, Anca & Niculcea, Tiberiu & Ranaweera, Pasika & Le-Khac, Nhien-An. (2020). Security Considerations for Internet of Things: A Survey. SN Computer Science. 1. 10.1007/s42979-020-00201-3.

[7] Hall, Fraser & Maglaras, Leandros & Aivaliotis, Theodoros & Xagoraris, Loukas & Kantzavelou, Ioanna. (2020). Smart Homes: Security Challenges and Privacy Concerns.

[8] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, Fourth quarter 2014, doi: 10.1109/COMST.2014.2320093.

[9] Jason R. C Nurse, Ahmed Atamli, Andrew Martin, Towards Usable Framework for Modelling Security Privacy Risk in smart home, 4th International Conference on Human Aspects of Information Security, Privacy and Trust in conjunction with the 18th International Conference on Human-Computer Interaction (2016), pp. 1-12.

[10] Huichen Lin and NeilW. Bergmann, IoT Privacy and Security Challenges for Smart Home Environments, Information DOI:10.3390/info7030044,(2016), pp. 1- 15.

[11] Gullapalli Sahith, Home Automation towards Security and Privacy to Accomplish as Smart Home Using Data Analytics, International Journal of Research in computer and communication Technology(IJRCCT), 6(12), 2017, pp. 347-351.

[12] Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* 2010, *54*, 2787–2805.

[13] Xu, L.D.; He, W.; Li, S. Internet of things in industries: A survey. IEEE Trans. Ind. Inform. 2014, 10, 2233–2243.

[14] Dr. Joy Iong Zong Chen, Kong-Long Lai “Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study” Journal of Soft Computing Paradigm (JSCP) (2020), Vol.02/ No.04 Pages: 236-245

[15] Drushti Desai1, Hardik Upadhyay, Security and Privacy Consideration for Internet of Things in Smart Home Environments, International Journal of Engineering Research and Development, 10(11), (2014), pp. 73-83.

[16] H. Manoj T. Gadiyar, Dr. Thyagaraju G. S., Bhavya T. P., Privacy and Security issues in IoT based Smart Home Applications, International Journal of Engineering Research & Technology (IJERT), 6(15), 2018, pp. 1-3.

[17] Tommaso Pecorella , Laura Pierucci, Francesca Nizzi, “Network Sentiment” Framework to Improve Security and Privacy for Smart Home, Future Internet, DOI:10.3390/Fi10120125, 2018, pp. 1-14.

[18] C.Ramakrishna, G.Kiran Kumar, A.Mallikarjuna Reddy, Pallam Ravi A, Survey on various IoT Attacks and its Countermeasures, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) 5(4), 2018, pp. 143-150.

[19] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin ZhaoA Survey on Security and Privacy Issues in Internet-of-Things, IEEE Internet of things Journal, 2017, pp. 1- 10.

[20] Eric Zeng, Shrirang Mare, Franziska Roesner, End User Security & Privacy Concerns with Smart Homes, Symposium on Usable Privacy and Security (SOUPS), 2017, pp. 1-16.

[21] Marlen S Bissaliyev, IoT: Security and Privacy in Future Home appliances, International Journal of Applied Engineering Research 12, 2017, pp. 10454-10457.

[22] Ali Dorri, Salil S. Kanhere , Raja Jurdaky and Praveen Gauravaram, Blockchain for IoT Security and Privacy: The case study of a Smart home, DOI: 10.1109/PERCOMW.2017.7917634, 2017, pp. 1-7.

[23] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson, On Privacy and Security Challenges in Smart Connected Homes, IEEE DOI 10.1109/EISIC.2016.21, 2016, pp. 172-174

[24] Sathish and Smys "A Survey on Internet of Things (IoT) based Smart Systems" Journal of ISMAC (2020) Vol.02/ No.04 Pages: 181-189, http://irojournals.com/iroismac/ DOI: https://doi.org/10.36548/jismac.2020.4.001

[25] Noura Aleisa and Karen Renaud, Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion), Hawaii International Conference on System Sciences HICSS- 50, 2017, pp.1-10

ISSN: 2582-3825 (online)
Submitted:02.12.2020
Revised: 10.01.2021
Accepted: 03.02.2021
Published: 17.02.2021