International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET2310229

Framework of Smarthome Automation and Security

M. Robinson Joel, G.Manikandan, Jose Saranish D, Jensing Samuel A. S, Kiruthika K, Balavasan S
Department of Information Technology, Kings Engineering College, Chennai, India

ARTICLEINFO

Article History:
Accepted: 01 April 2023
Published: 09 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
272-279

ABSTRACT

Numerous factors must be calibrated in accordance with the energy supply available to a smart home in order to schedule the functioning of household equipment. Due to the convenience and amenities it offers to homeowners, smart home automation is one of the current Internet of Things (IoT) applications that are gaining popularity. The NP-hard (nondeterministic polynomial time) problem of scheduling the operation of various appliances in a smart home, on the other hand, must be handled in polynomial time using an intelligent heuristic approach. In this piece of research, we put up the idea that wireless connectivity should be used to integrate sensors into household appliances so that owners can control them from a distance.

Keywords: IoT, Intelligent Heuristic Approach, Nondeterministic Polynomial Time, Smart Home, Security

I. INTRODUCTION

By effectively exploiting the benefits of communication technologies, the development of smart grid technologies tackles the majority of the issues relating to energy waste. The development of Internet of Things (IoT) technology in recent years has prompted the conversion of conventional homes into smart, connected homes. In a recent analysis by Cisco on worldwide internet development and trends, it was predicted that by 2022, there would be 28.5 million smart home devices. IoT devices in smart homes could provide hackers unauthorized access to observe tenants' private activities and use that information to their advantage. The development of a new technology known as microgrids addresses these problems. The connection between smart meters, load scheduling, and other systems is improved by micro-grids.

For instance, someone entering the house from a hot climate outdoors could choose a low power setting while another person within the house might switch on the air conditioner at a high power level. The user's interactions with their appliances in a smart home are also not taken into consideration by these scheduling techniques. For the existing HEMS systems to perform at their full potential, two-way communication between the HMES and the smart grid is required. Similar to this, scientists have lately employed a number of machine learning techniques to enable such two-way communication between the HEMS and smart grid.

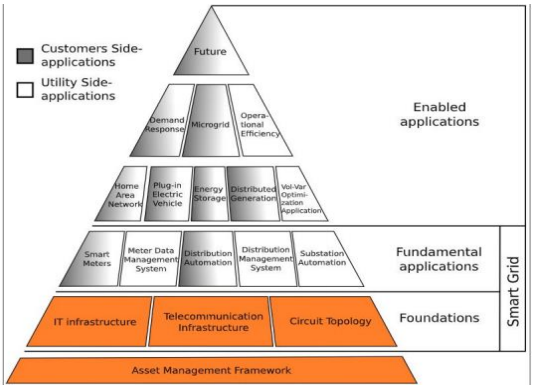

Figure 1. Smart Home Automation

Energy consumption

A certain day or week. To distinguish between these appliances, we split them into three categories: deferrable, non-deferrable, and controlled.

A. CATEGORY A: NON-DEFERRABLE HOME APPLIANCES

It is not possible to plan or move these appliances to a different day of the week or time of the day. A refrigerator is an illustration of this type of item. Given that a refrigerator must always be in the on position to prevent food and other objects from rotting, this is crucial. A television falls under the same classification as well. The TV cannot be used at a different time of the day or week. [3] Additionally, if any of the items in this category are planned for usage at a different time of day, they may make the user feel more uncomfortable. These appliances must always get the necessary energy, indicated by the symbol EA, in order to prevent continuous operation throughout the [1, 2, 3, , 24] hours of the day. Additionally, the user may only turn these appliances "ON." Figure 2 displays how much energy a refrigerator uses. The Figure demonstrates that when the refrigerator is turned on, there is a substantial energy usage [4].

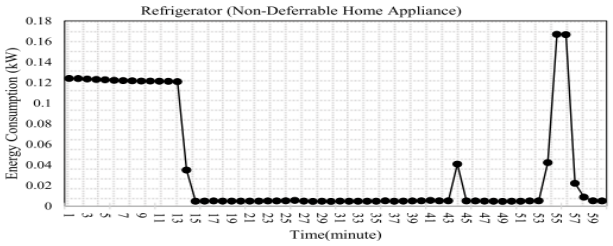

FIGURE 2 shows how much energy a refrigerator uses when operating at a lower level.

CATEGORY B: DEFERRABLE HOME APPLIANCES

These appliances can be moved or scheduled for use at a time of day when less energy is needed. For instance, if the amount of energy being used by the house exceeds the allowable amount, an item from this category can be moved to a different time of day or turned off. However, once a device of this type is turned on, it cannot be turned off until the process is finished. The user will feel more discomfort if these appliances are stopped while they are in use. Additionally, customers may only turn these appliances "ON" or "OFF" using two different operations. [9] The amount of energy used varies on the hours that they are running. Additionally, moving such items to a different time of day makes the user more uncomfortable. For instance, if a device of this type is moved from time t to time t + 3, where t is an hour, then the user must wait for three hours before using the device. [8] Therefore, these appliances not only use more energy but also make the user less satisfied. Such appliances' energy consumption is represented as E B n, t = OVn, t e B n, t, where OV is a Boolean variable that denotes whether the operation is on or off. A washing machine is one example of this kind of item. A washing machine should always be scheduled for off-peak hours in a smart home.

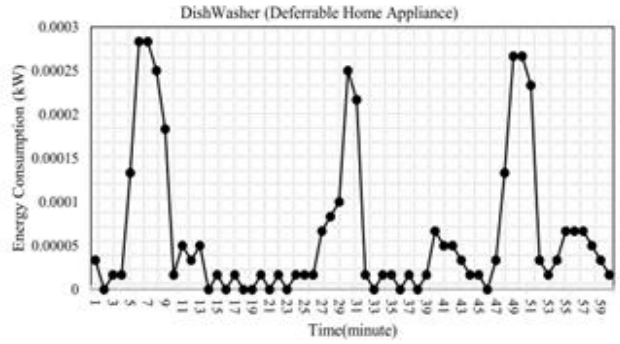

Figure 3 shows how much energy a dishwasher uses.

C. SMART HOME APPLIANCES SCHEDULING

Over the past 10 years, a single smart house scenario has been thoroughly researched.

Scheduling is mostly dependent on an appliance's ope rating duration in a single user smart home scenario with many appliances.

Typically, the hours in a day are used to split the entir e day into time intervals.

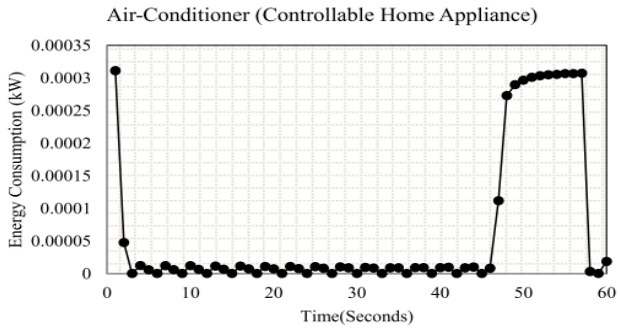

Figure 4 shows how much energy an air conditioner uses.

One of the main issues with employing LST is that it just ever completes the work at hand and never checks for upcoming jobs. The scheduling is modelled using historical data for all the variables needed by the LST method.

Smart home

Prior to entering the blockchain process, initial security checks have been performed on incoming requests to ensure confidentiality and integrity. Additional security has been introduced during the blockchain process to enhance data privacy and confidentiality and provide trustworthy TXs. This has a direct bearing on the degree of security desired in a smart home. Second, it would be required to investigate the waiting time of the transaction blocks in extreme circumstances where activity requests are submitted repeatedly at once from a single or numerous use

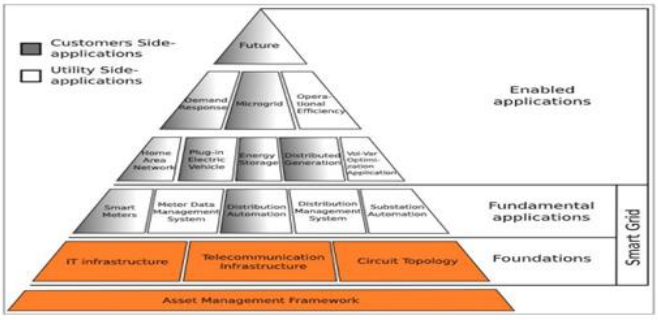

FIGURE 5. Smart Home Automation Contralable device

FIGURE 6. Smart Home

Smart homes detect which rooms you use and when in order to save energy. The system will monitor which rooms you are in and ensure that they are warm enough for you to utilize when you are there. Your house won't needlessly heat itself while you're away. The elegance of smart homes is that they don't try to coerce you into reducing your own energy

consumption. Instead, they monitor your way of life and look for ways to maximize the energy that is accessible. All of it makes it surprising that smart houses can occasionally save 30–40% on energy.

Smart homes conserve energy by monitoring when and in which rooms you use them, Solar panels are a terrific addition to your home. through the installation of solar panels on your roof and the connection of your smart home to them. Your smart house will develop self-sustaining capabilities where a smart home concept is the integration of different services within a home by using a common communication.

A private property that sends and receives data quickly is referred to as a smart home. It provides automated and intelligent services through a number of home products, including televisions, lights, and refrigerators. The human-free home-based communication system between gadgets and their environment includes these items [3]. Users manipulate the use of a variety of home devices in order to monitor and control themselves in line with user settings based on the network configuration of the house. IOT and the network environment are increasingly acknowledged as essential components of these smart homes. Particularly, in the network architecture of the smart home, which is mostly made up of embedded computers and is connected to various IOT devices based on the Internet [4], communication is shifting from wired to wireless. As opposed to how each user behaved.

With the advent of gateways, it is now possible to control additional devices within and outside of the smart home [5]. A more efficient and organized construction of the smart home network is projected to be achievable with the arrival of 5G, the next-generation mobile communication technology, as well as the convergence of several sectors.

Security

Modeling human behavior is a challenging task that requires several machine learning models to operate at once. Additionally, it is impossible to simulate human behavior in real-time because choosing the optimum course of action in every given typical scenario takes a lot of time. [13] Multiple IOT devices are connected to one another in smart homes, and these connections are channeled through gateways. Although gateways play an important role in smart homes, their centralized structure exposes them to a number of security risks, including those related to availability, certification, and integrity. In order to solve these security issues, we suggest a blockchain-based smart home gateway network in this study that provides defence against prospective gateway assaults on smart homes. The three layers that comprise the network are the device, gateway, and cloud layers.

Networks installed in smart homes collect and store a range of data, including personal data from the residents. The security of smart homes depends on this information being available only to authorized people. To guarantee the privacy of the smart home's features, we use blockchain in conjunction with an encryption technique.

Integrity: No data communication across configurations may be falsified while it is being sent or received.

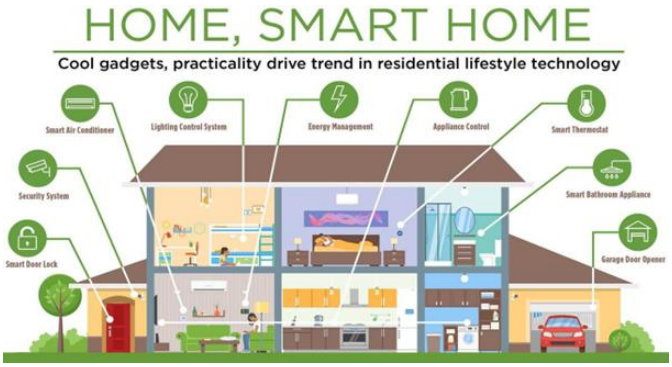

FIGURE 7. Home Smart Home

For example, let us take this message, “Alexa, Who’s Spying on My Living Room?”

You'll undoubtedly see a variety of devices that the residents of a smart house have placed for added convenience once you arrive. Smart TVs, Wi-Fi routers, smart speakers, thermostats, lightbulbs, and personal home assistants are just a few examples of these devices. However, these gadgets' internet access gives thieves a location to set up shop. For instance, the FBI has warned about the risks associated with smart TVs, noting that it is possible for hackers to enter into an unsecured set and take control, changing the channels, adjusting the volume, and even displaying inappropriate information to children. [7]

BLOCKCHAIN

One of the most important recent research reasons is blockchain at the moment. It is a cryptographically secure decentralized digital ledger that only allows appends. It offers a framework for trusted transactions (TXs) to be processed without the intervention of a third party. For verification purposes, each request has a record in the form of a chain of blocks and a digital signature. Blockchain stores tamper-proof and unchangeable information in a safe and encrypted way since the ledger is created and maintained by all system participants equally and there is no central server to administer the activity.

Blockchain holds unchangeable information in a safe and secured manner. The peer-to-peer (P2P) network that Blockchain uses allows any node—network user or new user—to join securely. A full copy of the blockchain is sent to any additional nodes or users that join the blockchain network. Every time a new request is made, a block is formed and delivered to every node in the network for confirmation to make sure it hasn't been tampered with. After then, the block is included in the chain of blocks. [2] The network's nodes reach a consensus to verify the block's validity as a whole. Each node in the network contrasts the blockchain it has with one it has received for verification.

Recently, a variety of industries, including banking, distribution, health care, and energy, have embraced blockchain technology. Blockchain was selected as one of the key technologies to lead the fourth industrial revolution period at the 2016 World Economic Forum. Blockchain has been selected as one of the top technological trends for 2017 by Gartner, Deloitte, and worldwide market research firms. [1] Blockchain is a well-known distributed ledger technology. It may be used to build a decentralized system that provides customers with a direct and active trust connection while overcoming the limitations of typical centralized systems' indirect and passive confidence assurances. Blockchain is easy to use and integrate in a number of enterprises, and the integrity of the block ensures the integrity of the data.

The another strategy makes use of a private blockchain, which is a permissioned blockchain that can only be accessed by pre-selected members of an established organization. The relevant authorities, which are the blockchain developers or ecosystem participants, pick these organizations. Consortium blockchain technology, which uses both public and private blockchain to construct blockchain, is the third method. According to, the consortium blockchain design is more suited for applications that need internal system supervision, transaction agility, and privacy protection. With the help of this blockchain technology, smart homes can now be guaranteed to be secure and private.[4]

Blockchain, which is based on a P2P network, links to an equal layer through every user, acting simultaneously as a client and a server. This can resolve the problem with a server-client architecture in a network system that is already in place and has several connected users that are controlled by a single server.

A shared digital ledger that contains data on network transactions makes up the foundation of blockchain. The Ledger is distributed to every member of the

network. A new transaction is considered authenticated if it has everyone's blessing.

Since ledgers record data as a hash value, any block's data that is changed or absent may easily be recovered. A ledger cannot actually be modified depending on the specifics of one transaction. It takes a minimum of 51% of all blocks being compromised at once to modify data. Thanks to distributed ledger technology, which is available to all network users, all new information is updated in real-time, and it is simple to trust and trace information.

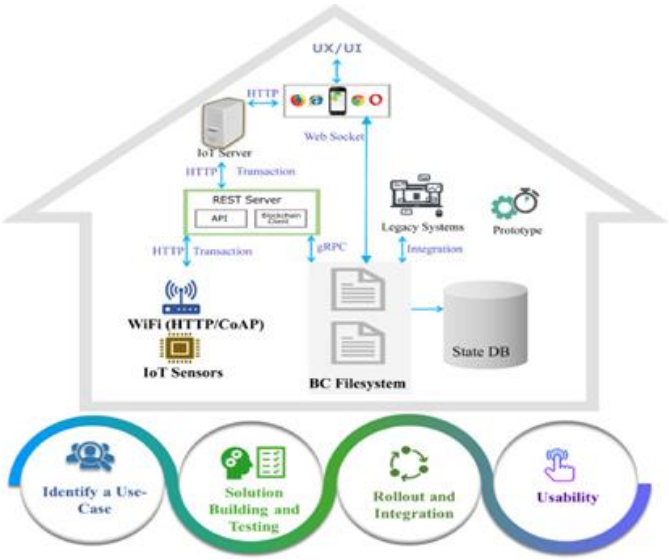

FIGURE 8. Smart Home Ecosystem

By eliminating intermediaries and relying on decentralized peer-to-peer networks instead of traditional centralized systems, transactions become more efficient and transparent. It creates a rapid and secure network environment for less money.

II. CONCLUSION

This study reviewed earlier research on the security of smart homes and took into account the findings by outlining a straightforward strategy for implementing a safe architecture that makes use of a polished version of the blockchain. [8] In just a few short years, the market for IoT devices has undergone significant changes. .The industry has expanded to include business companies that are working together to establish ecosystems, customised for mobile technology, which allows IoT devices to become networked, from starting with needy gadgets and no ecosystems to speak of. The notion of automating the house might have seemed bizarre and unrealistic at first, but as our devices grow smarter and more money is spent on the development of IoT consumer goods, we should expect to see rising competition stimulate more innovation in the field. In order to improve linked technologies in the burgeoning smart home sector, the third annual Smart Homes Summit is returning. [7] This year, the focus of the event is on how voice AI developments are driving service concepts for the home.

The research article mentioned above comes to the conclusion that wireless technology is used in every home automation system technique. Home automation methods based on Arduino, GSM, and Android have been established to make it simple for consumers to operate their appliances at home. A thorough breakdown of the various home automation techniques employing Arduino, GSM, and Android is provided together with their design, implementation, and flowcharts.

In order to achieve minimal energy use and reduce user pain in a smart home scenario, we simulated human appliance interaction using reinforcement learning. To teach the agents connected to each home appliance to conduct activities like as turning on, shutting off, and altering power levels in accordance with the maximum energy consumption restriction, the well-known learning algorithm known as the Q learning is utilised. [11] The whole day is further divided into twenty-four slots so that the home appliances may be scheduled for each hour. To optimally plan the deferrable, non-deferrable, and controlled appliances, the time slots are further divided into three groups: 1) peak, 2) semi-peak, and 3) off-peak. To develop agent coordination with one another, one agent shares the activities taken with the other agents. The recommended plan scheduled the

household appliances with the least amount of energy consumption and the least amount of pain for the smart home user, according to the performance study. [8]

The simulation findings are contrasted with those from our earlier research on scheduling home appliances. A deep Q learning method and artificial neural networks will be used in upcoming work to predict a multiple home user situation. [9] The operating time of each household appliance in the whole smart community will be scheduled using the agents of the community's smart houses. Additionally, an edge computing paradigm will be used to manage the entire home's communication from the edge.

III. REFERENCES

[1]. W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IOT services through software defined networking and edge computing: A comprehensive survey," IEEE Commun. Surveys Tuts., early access, May 26, 2020, DOI: 10.1109/COMST.2020.2997475.

[2]. Cisco Visual Networking Index (VNI), Complete Forecast Update, 2017–2022. Accessed: May 7, 2020. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/network-intelligence/serviceprovider/digital-transformation/knowledge-network-webinars/pdfs/1211_ BUSINESS_SERVICES_CKN_PDF.pdf

[3]. Competition is Increasing to Be the IOT Gateway to the Connected Home. Accessed: Jun. 21, 2019. [Online]. Available: https://www.gartner.com/[8]l8i[0]009en/newsroom/press-releases/2015-08-06-gartner-says-competition-isincreasing-to-be-the-IOT-gateway-to-the-connected-home

[4]. Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IOT) of smart home: Privacy and security," Int. J. Comput. Appl., vRol. 182, no. 39, pp. 3–8, Feb. 2019.

[5]. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IOT security: An exhaustive survey on IOT vulnerabilities and a first empirical look on Internet-scale IOT exploitations," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[6]. T. Alladi, V. Chamola, B. Sikdar, and K.-K.-R. Choo, "Consumer IOT: Security vulnerability case studies and solutions," IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 17–25, Mar. 2020.

[7]. B. Zhou, W. Li, K. W. Chan, Y. Cao, Y. Kuang, X. Liu, and X. Wang, "Smart home energy management systems: Concept, configurations, and scheduling strategies," Renew. Sustain. Energy Rev., vol. 61, pp. 30–40, Aug. 2016.

[8]. B. Celik, R. Roche, S. Suryanarayanan, D. Bouquain, and A. Miraoui, "Electric energy management in residential areas through coordination of multiple smart homes," Renew. Sustain. Energy Rev., vol. 80, pp. 260–275, Dec. 2017.

[9]. I. Abubakar, S. N. Khalid, M. W. Mustafa, H. Shareef, and M. Mustapha, "Application of load monitoring in appliances' energy management—A review," Renew. Sustain. Energy Rev., vol. 67, pp. 235–245, Jan. 2017.

[10]. H.-T. Roh and J.-W. Lee, "Residential demand response scheduling with multiclass appliances in the smart grid," IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 94–104, Jan. 2016.

[11]. B. Silva, M. Khan, and K. Han, "Load balancing integrated least slack time-based appliance scheduling for smart home energy management," Sensors, vol. 18, no. 3, p. 685, Feb. 2018.

[12]. A. Mukherjee, P. Mukherjee, N. Dey, D. De, and B. K. Panigrahi, "Lightweight sustainable intelligent load forecasting platform for smart grid applications," Sustain. Comput., Informat. Syst., vol. 25, pp. 1–18, 2020.

[13]. F. Pallonetto, M. De Rosa, F. Milano, and D. P. Finn, ‘‘Demand response algorithms for smart-grid ready residential buildings using machine learning models,’’ Appl. Energy, vol. 239, pp. 1265–1282, Apr. 2019.

[14]. Lee, Y., Rathore, S., Park, J.H. et al. A blockchain-based smart home gateway architecture for preventing data forgery. Hum. Cent. Comput. Inf. Sci. 10, 9 (2020). https://doi.org/10.1186/s13673-020-0214-5.

Cite this article as :

M. Robinson Joel, G.Manikandan, Jose Saranish D, Jensing Samuel A. S, Kiruthika K, Balavasan S, "Framework of Smarthome Automation and Security", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 2, pp. 272-279, March-April 2023. Available at doi : https://doi.org/10.32628/IJSRSET2310229
Journal URL : https://ijsrset.com/IJSRSET2310229