Securing the Smart Devices in Home Automation System

Syeda Sabah Sultana and J. Sangeetha

Abstract Security is the major concern in every infrastructure such as offices, banks, hospitals, etc. Due to lack of security in the existing home automation system, hackers can easily access and collapse the system. Hence, in this research work, we are providing security to the remotely controlled home infrastructure and to reduce the energy consumption of smart devices. The smart device consists of the appliances such as four lights and two switches operated using the web-based application. This application allows only authorized users to remove these smart devices which are not in use for longer time and also the hacked devices. Thus, we are reducing energy consumption and securing our smart devices from hackers. Adding to the benefit of the user, through this application we can change the status of the devices either to on or off state. The status of the devices is stored in the cloud in the encrypted form (ciphertext) using the encryption technique such as the AES algorithm. Through the server using Wi-Fi module, this ciphertext can be accessed by the user credentials and decrypt it through web-based application. In this research work, major security issues like authentication and verification are taken care, and this work focus is on reduction of energy consumption by removing unnecessary devices and protecting the smart devices from hackers in the existing home automation system.

Keywords Internet of Things · AES algorithm · Energy consumption · Verification · Authentication

1 Introduction

The Internet of Things interconnects digital devices across Internet into everyday devices that enable them to send and receive data. It plays an important role in our daily lives. The Internet of Things contributes too many areas such as education,

S. S. Sultana (✉) · J. Sangeetha
Department of Computer Science and Engineering, M S Ramaiah Institute of Technology, Bengaluru 560054, India
e-mail: syedasabah.01@gmail.com

D. P. Agrawal et al. (eds.), *Cyber Security, Privacy and Networking*, Lecture Notes in Networks and Systems 370, https://doi.org/10.1007/978-981-16-8664-1_24

health system, automobiles, entertainment, smart home, etc. It has many challenges such as security threats, data leakage, data manipulation, and other vulnerabilities [1].

In [2], the approach to machine learning (ML) [2] is showed that accelerometer data is used to trade in with problems with Gesture Recognition (GR). Objectives of the approach are to provide classification with high accuracy that are typically independent of the user and devices, independent and system orientation for home automation systems, a heterogeneous scenario in earlier GR literature; this was not thoroughly explored.

In [3], simplistic simulation of a full home automation system has been carried out in using components and raw materials that are readily available. The system automates five separate devices/loads that can be accessed via an Internet connection through a webpage from anywhere in the world. With a login function, the webpage thus given is protected. A revolutionary utilization monitoring feature, which monitors the length of use of and system after each ON-OFF cycle, has been established. It allows consumer to monitor and reduce use, energy utilization and therefore effectiveness bills strategically.

In [4], it present a new intelligent smart home concept that incorporates the IoT concept based on a web application. In addition, a communication model is specified for exchanging data in the same medium. It provides a common medium for all heterogeneous devices to communicate. In addition, based on web applications, device architecture is also proposed. To send or receive action messages over the network, the web application concept is used. The architecture presented offers the aspects of implementation, study and visualization in which different devices interact with other devices. Similarly, energy usage is also computed for the sensors installed in the proposed smart home. The energy consumption of the sensors using the architecture proposed is substantially less. The final assessments of the network architecture meet the user-related needs, whether the input data is real time or offline when taking real-time action.

The author [5] introduces smart home and security system scheme, also in brief present the system's architecture, system's functionality, interface of system, identity addressing and security mechanism. In this system, sensing and home gateways allow connecting network of all levels allowing users to query data at any instance, controlling of devices on home network. The system's performance is measured. As sensing technologies advance, more study focuses on increasing the efficiency of the system and security framework of the system to satisfy the requirements of users' privacy.

In [6], in order to control switch-based appliances through human speech, there are human perception problems that comes from human speech. Also the missing of necessary parameters is a problem to understand for identifying an object by a computer. To overcome the inherent issues, context information is employed. Through this, it can provide indication to understand human speech to be used as a control command for home appliances. Thus the paper concludes with the monitoring of proposed control system by sensors. Context information previously inferred or a user at home can monitor the system.

In [7], the existing network infrastructure IoT allows devices to remotely control. IoT allows these devices to be incorporated into computer-based systems, resulting in increased performance, precision and cost savings while requiring less human interaction. Cyber-attacks harm other devices if they are secured poorly, and they use them as gateway which results in security and privacy issues in the network. The author focuses more on the constraints and security challenges. It concentrates on the challenges gained by the IoT-connected devices as well as their capability to connect. Also communication between the devices and remotely managing of large number of automated devices via the Internet.

In [8], numerous elements are contained in an IoT solution that effects the execution of security and privacy features which brings a functionality concern. Some elements such as open-source and proprietary are also among those that users are unable to control them. However, a smart home device can be controlled by user via application of smart home remotely. This consists of embedded devices linked to the cloud. To grant digital entity, a lightweight identity stack is proposed for IoT with the devices and users that interact with them. An authentication scheme is used for Fast Identity Online (FIDO). Every time a FIDO authentication receives request from the user, a keep-alive protocol is used.

In [9], there are many key challenges in IoT objects, IoT objects need simple security solutions that mostly function at minimum energy levels and with lesser amount of capabilities thus resulting in hindrance of difficult security solutions. This hindrance is caused due their memory and computational requirements such as cryptographic protocols. One way of securing devices against emulation attacks is the use of environmental-based fingerprinting. To authenticate devices, device fingerprinting is a technique that uses unique features extracted from the objects transmitted signals and environment.

In [10], the author focused on an authentication scheme on IoT devices. To support the authentication, all set of devices communicates with a gateway. There is connection between controller and the gateway which can access to the central data. The access can be provided by passing the authentication scheme through gateway and controller. There are three levels where the message flows between: things, gateway and the controller. The first phase requires obtaining a public key certificate by a gateway through the controller. The second phase starts by thing by sending an authentication request to the gateway. The last stage is requisition of authentication from IoT device to gateway. Testing is completed by the tool AVISPA. Evaluation of result shows the identity-based authentication scheme is opposed to various attacks.

The author [11] explains that RFID is vulnerable to attacks on security and privacy. This is because any request via wireless communication from a reader, the RFID responds to its unique ID. Due to the non-selective response of RFID tags to all reader queries, the items recognized with tags may reveal information that is insightful. Through this, the adversary can attain trace goals rely. Physical attacks, cheat tags, DoS attacks, eavesdropping and communication flow analysis and other security issues are all faced by RFID systems. Tag reading by attackers can be executed without suitable control solutions. Thus, the functionality of each application has been more focused by users.

For end-user appliances, the Home Energy Management System (HEMS) is presented through hardware demonstration [12]. The contact delay time of the HEMS used to perform load control and consumption of energy are investigated in detail.

The objective of this research work is to focus on the challenges of IoT concerning security and privacy. The main purpose of this work is to provide security to the devices in the existing smart home system and to reduce the consumption of energy used by these devices. The system consists of the appliances such as four lights and two switches. It is operated using web-based application. The application allows removing the devices which are not in use for longer time in order to reduce energy consumption and to protect the devices which are hacked by the hackers. It also allow to change the status of devices to on or off state. The status of the devices is stored in the cloud in the encrypted form. An AES algorithm of 128 bit is used as the encryption technique that generates the ciphertext. Through the server using Wi-Fi module, this ciphertext can be accessed by the user credentials and decrypt it through web-based application. In this research work, major security issues like authentication and verification are taken care and this work focus is on reduction of energy consumption by removing unnecessary devices and protecting the smart devices from hackers in the existing home automation system.

The system provides security to the existing system in two levels: In the first level, the credentials are verified by the server that comes from the user for the authentication, and the second level is to provide verification through the generated OTP (One Time Password) and notifies the user through an e-mail in case of animosities such as manipulation of data or the hacker trying to hack the data. This paper aims to shed light concerning security requirements: authentication, confidentiality in existing home automation system. Further, the organization of the paper is as follows: Sect. 2 explains the methodology of the proposed system, Sect. 3 gives the exemplar of AES algorithm, and Sect. 4 provides results of the proposed model and finally the conclusion is discussed.

2 Proposed Methodology

In this research work, we have considered the following hardware module: Arduino UNO, Raspberry Pi, Wi-Fi module (Node MCU) and Relay module. The hardware design in our existing automation system consists of devices (i.e., four lights and two switches). For the better understanding and security of these devices, they are identified with device identifiers (IDs) with the naming convention as in Table 1.

The connection between client and server is formed through the activated Wi-Fi option available in the smartphone. Raspberry Pi acts as a server side. The Internet Protocol (IP) address is configured to the Virtual Network Computing (VNC) viewer to connect to the Raspberry Pi. The Arduino Uno board consisting of digital pins is connected to each IoT device in the system. Each system is connected via relay to the arduino. A Python program loaded onto the Arduino Uno board's microprocessor

Table 1 Device name and identification of the devices

S. No.	DeviceName	DeviceID
1	Light1	SS01
2	Light2	SS02
3	Light3	SS03
4	Light4	SS04
5	Switch1	SS05
6	Switch2	SS06

chip helps to perform action when particular input is received. End-user web-based application is used to monitor and control the smart devices from any remote location.

The software module consists of the web-based application and cloud solution. A web-based application provides user a user interface. Every user needs to register with username and password. The application provides two levels of securities. In the first level of security, when IoT devices are accessed by the user, it sends requests to the server using their login credentials and this is authenticated by the server. These credentials are stored in the server. For authentication, the server verifies the information provided by the user such as email address, password. When the attacker makes many failed login attempts, i.e., up to three attempts, an email is sent to the real user requesting that they change their password immediately. In the second level of security, the user's identity will be verified through the use of an OTP. The user can then modify the status as on or off state of the devices via the cloud. Here the status of device 'on' is considered as 'yes' and 'off' as 'no'. The application can remove the devices once the two-level securities have been successfully completed. It allows you to periodically update your profile and change your password. This application is used to modify a device's status from its prior state. It is encrypted and saved in the cloud as ciphertext. As a result, the ciphertext produced uses the AES algorithm which is an encryption technique.

3 AES Algorithm Explanation

The encryption technique is implemented using AES algorithm. The AES algorithm is a symmetric-key cipher that encrypts the data using a single key shared by both sender and recipient. The AES algorithm here uses the Shift-Row Transformation technique to generate the ciphertext.

Let us understand with an illustrative example, where the plaintext is 'Yes'. Converting the plaintext into Hexadecimal form, we have the values for 'Y' as 59, 'e' as 65, 's' as 73 and for 'whitespace' as 20. Hence considering the entire plaintext with space up to 16 bytes, the hexadecimal value for the plaintext is

59 65 73 20 20 20 20 20 20 20 20 20 20 20 20 20

Consider the key Dd_WFBROXfRbaHUX for round 0 key.

Converting the key into hexadecimal form, we have the values as: for ‘D’ the hexadecimal value is 44, for ‘d’ is 64, ‘_’ is 5F and so on the values goes on for the rest of the bytes in the key.

The final hexadecimal value for the key is:

44 64 5F 57 46 42 52 4F 58 66 52 62 61 48 55 58

Key expansion process is used by AES algorithm to create round keys for each key. It is created word by word in an array form. Each word consists of 4 bytes. The following are the steps to be followed:

Step 1: First four words (w0, w1, w2, w3) are generated from the key; each word consists of bytes w[0] = (k0, k1, k2, k3), w[1] = [k4, k5, k6, k7], w[2] = [k8, k9, k10, k11] and w[3] = [k12, k13, k14, k15].

Here in our algorithm, the following are the words consisting of 4 bytes.

$$\text{w}[0] = (44\ 64\ 55\text{F}\ 57)\ \text{w}[1] = (46\ 42\ 52\ 4\text{F})$$

$$\text{w}[2] = (58\ 66\ 52\ 62)\ \text{w}[3] = (61\ 48\ 55\ 58)$$

Copying the last four bytes of the existing key to a four-byte temporary vector

$$\text{w}[3] = (61\ 48\ 55\ 58)$$

Step 2: Circular byte left shift
It takes a word w[3] of 4 bytes and perform shift operation each byte to the left as shown below

w[3] : (48 55 58 61)

Step 3: Byte Substitution (S-Box)
This step relies on nonlinear S-Box. In this step, a byte in the state is replaced to another byte which is called as Rijndael S-box.

(S-Box) for w[3] : (52 fc 6a ef)

Step 4: Adding round constant RCON
Each RCON is a four-byte value, where the rightmost 3 bytes are always 0 where

$$\text{RCON}[i] = [x \wedge i - 1,\ 00,\ 00,\ 00]$$

The values $x \wedge i - 1$ are to be computed in the same representation of Galois field (GF)

$$(\text{GF}) = (2 \wedge 8)$$

Since we are calculating key for round 1, we need the RCON value as RCON[1] = [01, 00, 00, 00]

g(w[3]) = RCON[1] XOR w[3]

g(w[3]) = (01 00 00 00) XOR (52 fc 6a ef)

g(w[3]) = (53 fc 6a ef)

w[4] = w[0] XOR g(w[3])

w[4] = (44 64 55F 57) XOR (53 fc 6a ef)

w[4] = 17 98 35 b8

w[5] = w[4] XOR w[1]

w[5] = 51da 67 f7

w[6] = w[5] XOR w[2]

w[6] = 9 bc 35 95

w[7] = w[6] XOR w[3]

w[7] = 68 f4 60 cd

The first round key generated is (17 98 35 b8 51 da 67 f7 9 bc 35 95 68 f4 60 cd). Similarly, we can generate for the remaining nine rounds using AES algorithm.

There are lots of attacks done by the eavesdroppers. One of the popular attacks is the brute-force attack, a method of trial and error in order to get the original data. The AES algorithm is computationally secure than Data Encryption Standard (DES) against this attack because it is not possible to acquire 128 bit key to get attacked.

4 Results Analysis

In this research work, two levels of security are implemented: authentication/authorization of the system and verification/validation of the system.

The first level of security, which is especially important from a system-wide perspective, is the authentication and user authorization. The result analyses are explained in detail.

In the first level of security, the user must first register with the Smart Home Automation System by entering his or her information such as Name, Email-ID, Phone Number and Password on the Sign-In page. The user is authorized to input the password that is saved in the server once the Email ID has been registered. When a user logs in using his or her registered credentials (username and password), the server verifies the user identification whenever the user logs in with the registered credentials, i.e., username and password. If the entered password is incorrect three times in a row, a login alert is sent to the registered Email-ID, requesting that the password be changed immediately. This assures that the user's credentials are secure and that no attacker may mislead the information and uses it for malicious attacking the system. As a result, the IoT devices are safe and inaccessible to attackers. Thus, the system allows the user to change their password to a new one. Passwords should be changed on a frequent basis to keep the system secure. The system has a functionality that allows you to update your profile. This feature allows you to modify your profile and password. Users can update their profile by changing their name and phone number.

In the second level of security, the server verifies the user's identity by requiring the user to enter a four-digit One Time Password (OTP). An OTP is sent to the user's registered email address. The server allows access to the system based on the user's identification. After a successful login, a web page providing complete control of the system is displayed.

From Figs. 1 and 2, we can observe that the user uses the system to turn the lights and switches such as Light1, Light2, Light4, Switch1 in on state and to turn the light and switch such as Light3 and Switch2 in off state.

4.1 Removing of Devices

The system provides an additional feature of removing devices from the system. The user has the flexibility of removing devices when they are no longer required by

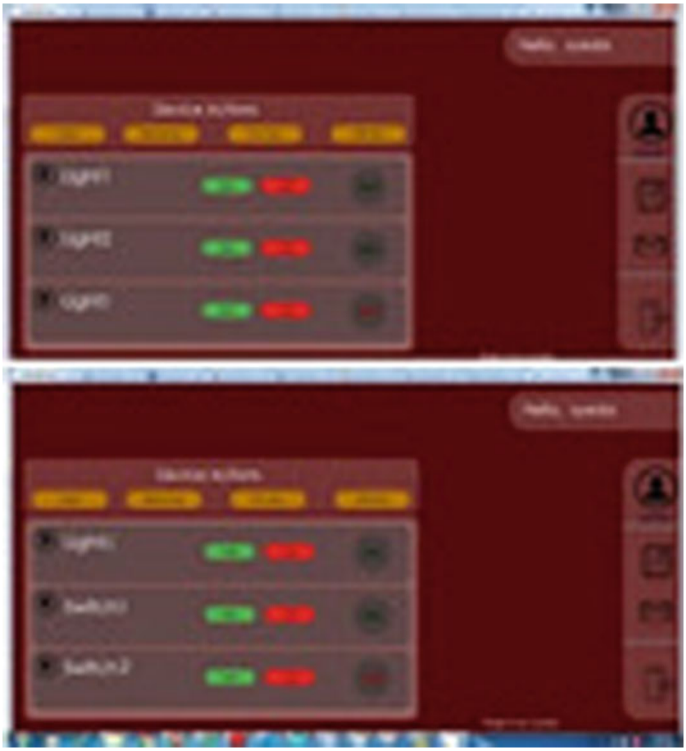
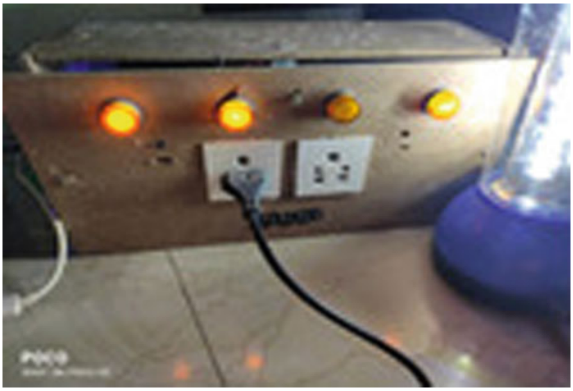


Fig. 1 User interface for operating the devices

Fig. 2 Output status of devices (i.e., Light, Light2, Light, Light4, Switch1, Switch2)



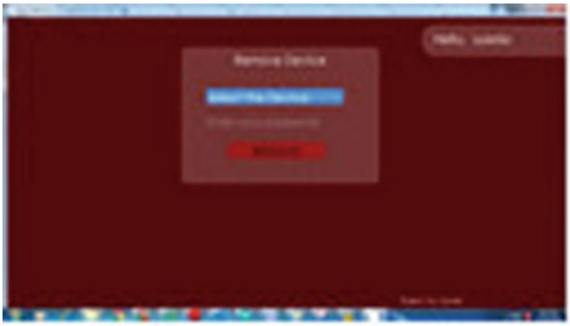


Fig. 3 Removing of device successfully

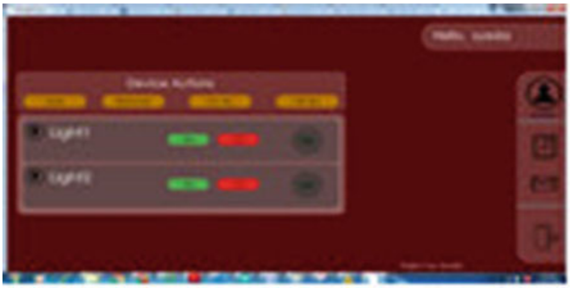


Fig. 4 After successfully removing of device

selecting the device and entering the correct password as shown in Fig. 3. The alert message is shown on removing of device successfully.

Assume we have 3 devices Light1, Light2, Switch1, we can observe that device "Switch1" is removed successfully from the application as shown in Fig. 4.

On successful removing of device, an email is sent to the registered user's Email-Id as shown in Fig. 5.

Also, it is necessary to remove unnecessary devices that are no longer used as this will consume energy. The device can be removed using the remove device option from the system. This helps reduce energy consumption and also care is taken, wherein

Fig. 5 Email on removing of device

only concerned person will be allowed to remove the devices. In this way, two-layer security is provided, in which the first level of security requires user to enter correct password for removing the devices and the second level of security which notifies the user through email whenever the device is removed from the application.

There are also larger chances of the devices getting hacked by the hacker, and the removing of device functionality provides security to the system by removing the device.

4.2 Cloud-Based Solution

In this research work, a secure cloud-based is employed as the solution. It allows IoT devices to connect and communicate with one another. Because of the limited resources available in IoT, a substantial amount of data generated by IoT devices must be communicated to the cloud, and all devices must be accessible through the Internet. Because users have little control over their cloud services, they must trust their cloud providers to provide adequate security methods for their data. As a result, encryption is used in this approach. As a result, the encryption utilized in this approach ensures that end-to-end communications are secure.

For instance, in the existing system, the input data/plaintext we considered were the on or off status of devices. The statuses ‘on’ and ‘off’ have been interpreted as ‘yes’ and ‘no,’ respectively. This information is obtained from the Arduino board and is used in the encryption process.

Consider Device ID SS01, the input data/plaintext is the status of devices on or off. This information is received from the Arduino board. Let AC be the state of device, Y is called the active, and KY represents the key which is being used to perform addition of matrix.

In this research work, 128-bit key size is utilized. The key calls for ten rounds. The number of rounds is determined by the key size utilized. The ciphertext generated for the individual device ID in the cloud is represented by CT. We may also produce ciphertext for other devices using their unique device IDs.

The user can access the cloud to change the status (ON/OFF) of the devices in this existing system. For each device ID such as SS01, SS02, SS03, SS04, SS05, SS06, the algorithm generates a unique ciphertext which is stored in the cloud whenever the user changes the device status from on to off or vice versa. As a result, the confidentiality between sender and receiver is preserved.

Furthermore, data encryption is essential, because we are using the open source Firebase cloud, an attacker can obtain the device’s system information without the user’s consent or awareness. These aid attackers in deciphering patterns of user behavior in order to track devices. Because an attacker can remotely change the status of the devices, posing a threat to the user’s devices.

Assume we’re accessing and changing the state of devices via a public network outside of our home, such as Wi-Fi in a mall, train station or other public location.

An attacker with access to data stored in the cloud can intercept this communication between the devices and the cloud. As a result, data saved in the cloud and IoT devices are secure, and no attacker can access them.

5 Conclusion

In this paper, we have discussed security and energy consumption as the major problems in the existing smart system. If any device is hacked by the attacker, it will provide the user with an alert mail on their respective credentials which can protect the system. The AES algorithm aids in the generation of cipher text, which is used to securely store data in the cloud. It also ensures that the cloud is secure, where the status of the devices is stored in encrypted form so that no attacker should be able to change the state of the device. The system also focuses on the second major problem of reduction of energy consumption by the devices. The functionality of removing device provides user to remove unnecessary devices which are not in use for longer time and the hacked devices. Thus, reducing the energy consumption and securing the smart devices from the hacker.

Acknowledgements We would like to thank M.S Ramaiah Institute of Technology, Computer Science and Engineering for supporting this research work.

References

1. Granjal J, Monteiro E, Sá Silva JS (2010) A secure interconnection model for IPv6 enabled wireless sensor networks. In: IFIP wireless days, Venice, pp 1–6
2. Cenedese A, Susto GA, Belgioioso G, Cirillo GI, Fraccaroli F (2015) Home automation oriented gesture classification from inertial measurements. IEEE Trans Autom Sci Eng 12(4):1200–1210. https://doi.org/10.1109/TASE.2015.2473659
3. Paul S, Indragandhi V, Kumar NK, Raja Singh R, Subramaniyaswamy V (2019) An IoT based home automation system. IOP Conf Ser Mater Sci Eng 623:012014. https://doi.org/10.1088/1757-899x/623/1/012014
4. Khan M, Din S, Jabbar S, Gohar M, Ghayvat H, Mukhopadhyay SC (2016) Context-aware low power intelligent smart home based on the Internet of Things. Comput Electr Eng 52:208–222. ISSN 0045-7906
5. Ting J, Yang M, Zhang Y (2012) Research and implementation of M2M smart home and security system. Secur Commun Netw 8. https://doi.org/10.1002/sec.569
6. Han Y, Hyun J, Jeong T, Yoo J-H, Hong JW-K (2016) A smarthome control system based on context and human speech. In: 18th international conference on advanced communication technology (ICACT)
7. Balamurugan S, Ayyasamy A, Suresh Joseph K (2018) A review on privacy and security challenges in the Internet of Things (IoT) to protect the device and communication networks. Int J Comput Sci Inf Secur (IJCSIS) 16(6)
8. Chifor B-C, Bica I, Patriciu V, Pop F (2018) A security authorization scheme for smart home Internet of Things devices. Future Gener Comput Syst 740–749

9. Sharaf-Dabbagh Y, Saad W (2016) On the authentication of devices in the Internet of Things. In: IEEE 17th international symposium on a world of wireless, mobile and multimedia networks (WoWMoM), June 2016, pp 1–3
10. Salman O, Abdullah S, Elhajj IH, Chehab A, Kayssi A (2016) Identity-based authentication scheme for the Internet of Things. In: IEEE symposium on computers and communication (ISCC), June 2016, pp 1109–1111
11. Feng H, Fu W (2010) Study of recent development about privacy and security of the Internet of Things. In: International conference on web information systems and mining, Sanya, pp 91–95
12. Kuzlu M, Pipattanasomporn M, Rahman S (2012) Hardware demonstration of a home energy management system for demand response applications. IEEE Trans Smart Grid 3(4):1704–1711. https://doi.org/10.1109/TSG.2012.2216295