A Literature Review of IoT Technologies for Home Automation

Submitted by,
Names and IDS

Prepared in partial fulfillment of EEE F411 Internet of Things

Under guidance and supervision of

Dr. K R Anupama
Assistant Professor, Department of EEE,
BITS Pilani KK Birla Goa Campus

February 23, 2021

Contents

1 Introduction

talk briefly about different IoT applications and in more detail about home automation in particular.

2 Smart home systems

mention briefly about each domain and what we aim to explore

3 Healthcare Smart-Homes

3.1 Introduction of SH as layers:

3.2 Sensing Technologies:

3.3 Communication Layer

3.4 Data processing, recognition

3.5 Human computer interaction

3.6 Overview of implementations

4 Security systems for smart homes

With the advent of smart homes, due to increased connectivity between a home system and many other large-scale systems, it is important that no malicious softwares enters the system and causes any kind of corruption. Let us consider this with the example of smart homes and smart grids. An energy aware household is expected to optimize the power budget used whilst also not slacking on comfort of the residents. This requires communication not only with the smart grid and the house, but also within all entities in the smart house. With all the communication depending on Information Technology, the system becomes vulnerable, which if exploited could not only damage the infrastructure of the home system but also the Smart Grid, which will have a large-scale impact. This also means that with the rise in Smart Grids, the role of Smart Homes and their residents becomes increasingly important.

4.1 6 Aspects of System Security

The following are the 6 aspects which are used while considering security of a system:

1. Confidentiality: only authorized personnel should have access to the data
2. Integrity: assurance that the accuracy and consistency of the data is maintained. Any and all changes in the data are detected.
3. Availability: Any network resource should be available to authorized entity.
4. Authenticity: of the communicating parties involved i.e., all communicating parties must be validated and the information sent by them must indeed be sent by them
5. Authorization: access control of each entity must be defined in the network.
6. Non repudiation: undeniable proof should exist for any claim of any entity

4.2 Impact Evaluation

Any security attack can be divided into categories based on whether the attack affects the system:

- Passive: Here the threat is only attempting to take information from the system network, without affect its resources. This information could be valuable and be used in different ways to plan a more disastrous attack. In dealing with such attacks, one focuses on prevention rather than detection, as that can be very tough.
- Active: Here the attack actively attempts to damage/affect the system network resources or operation. The most common amongst these attacks are masquerading, replay, message modification, denial of service and malicious software.

Now based on the impact of the attack to the system, the FIPS 199 standards can be used categorizing the attacks as Low level, Moderate level and High level, which in themselves fairly explain their damage extents.

The architecture of the Smart home system is divided into internal and external systems, where, in this case, the Energy Service Interface (ESI) is in contact with the smart grid, and manages communication with the external system. And the Energy Management System (EMS) manages the internal system.

4.3 An outline of the assumed architecture

The architecture of the Smart home system is divided into internal and external networks, where, in this case, the Energy Service Interface (ESI) is in contact with the smart grid, and manages communication with the external system. And the Energy Management System (EMS) manages the internal system.

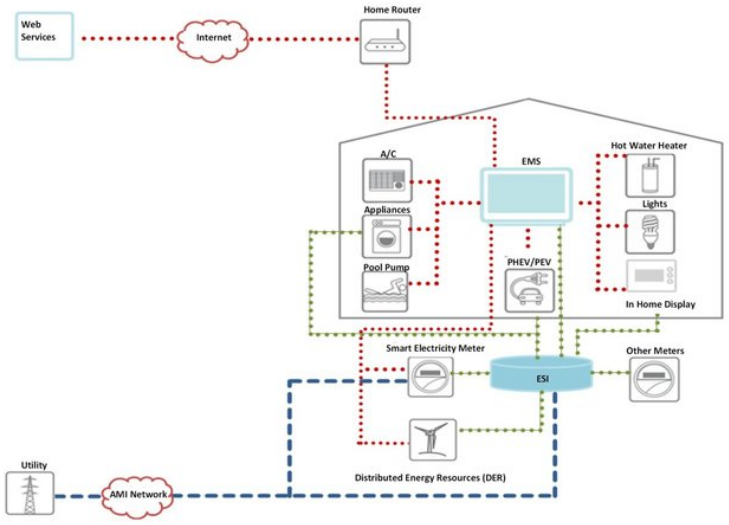

Figure 1: An overview of a Smart Home's architecture, internal and external environments.[12]

4.4 Smart Home Attacks

Broadly categorizing, the major possible attacks possible on the Smart Home system are in the following ways, when considered with regards to communication with a Smart Grid:

SH1) Attacks threatening successful device energy-consumption reporting – When energy consumption of data is collected at very short intervals, eavesdropping on such an information could be used to infer a lot about the lifestyle of the residents, hence create a major risk to privacy. Needless to say, how this data can be used to plan a more severe attack on the resident (e.g.: burglary, kidnapping). In the same place if it is managed to send false, or replayed data to the EMS, a false extra financial burden can be created for the consumer. This could also be achieved by impersonating the EMS rather than only "piggybacking" the network. (Generally low impact)

SH2) Attacks aiming Energy Import/Export signal at ESI - As the ESI is an entity in direct communication with the grid, any kind of message modification in the import export communication at a large scale could significantly impact the grid. Repudiation is also an important threat under this scenario since we expect the customer to be collaborating with an ESP for the management of his DERs due to his lack of experience. In such a case the customer should not be able to suggest that his ESP did not react when it should have/ or reacted when it shouldn't have. (Generally moderate Impact)

SH3) Physical meter tampering/reversal or removal – Mischievous customers try to tamper with the meter to decrease the bill, which needs to be stopped. (Generally Low impact)

SH4) Attacks against remote home monitoring and control – These basically include attacks where-in an adversary may impersonate the customer to control the devices in different ways (either switching on/off all devices or maybe modifying the messages). These attacks could have a low impact or may even be life threatening depending on the device(s) being abused. There is also the case of device impersonation where the commands sent remotely by the user are somehow directed to a device other than they were intended for. Therefore, Non-repudiation becomes a major factor in dealing with such attacks.

SH5) Attacks aiming the request for energy usage data -Eaves dropping on the detailed bill of energy consumption by the user is again a direct attack on the users' privacy, so this is another part where security protocols must be implemented. Table <1> gives a comprehensive list of the smart home security issues with respect to a smart grid. It can be used as a basis for analyzing issues possible whenever we include another system in our analysis.

Scenario :	Possible Threads	Security Goals Compromised	Degree of Impact
SH1	Eavesdropping (N) Traffic Analysis (N) Message Modification (N) Replay Attack (N) EMS Impersonation (SH)	Confidentiality Integrity Authenticity	L-M
SH2	Repudiation (N) Message Modification(N) Replay Attack (N)	Non repudiation Integrity Authentication	M
SH3	Tampering/Reversal/ Removal of Meter (SH) Illegal Software Modification/Update(SH)	Authentication Integrity	L
SH4	Customer Impersonation (N) Device Impersonation (SH) Message Modification(N) Replay attack(N) Repudiation(N)	Integrity Non repudiation Authentication	$L - H$
SH5	Customer Impersonation(N) Eavesdropping/Message(N) Interception (N) Message Modification(N)	Confidentiality Integrity Authenticity	L-M

Table 1: Smart Home Security Issues [12]

4.5 Security countermeasures

4.5.1 Confidentiality:

Cryptography is the most basic technique for achieving confidentiality. There are two types of cryptographic algorithms, Symmetric and Asymmetric. Symmetric algorithms (such as the standards AES and TDES) are expected to be used for the purpose of data encryption within the Smart Grid. Asymmetric algorithms on the other hand, (such as the approved RSA, DSA, ECDSA etc.) are expected to be used for the purpose of digitally signing messages.

4.5.2 Privacy:

With the deployment of smart meters, it is clear that through the data collected by the smart meter a lot could be known about the consumer, thus causing fear. Privacy can be achieved by the following ways: Anonymization: The data and its source have their link removed before the data reaches its destination for computation. Trusted Aggregators: Trusted third party can handle aggregation of metering data and its forwarding to the smart grid utility. Homomorphic Encryption Perturbation Models : Introduction of noise of known distribution Verifiable Computation Models Data Obfuscation Techniques: : Battery-based approaches that aim to conceal the amount of energy consumed by a premise by buffering or releasing their energy load.

4.5.3 Integrity:

One way to ensure integrity is using the cryptographic hashing techniques, which are designed for high integrity assurance in traditional networks. When using such techniques the sending side uses a hash function to compute the checksum of the message to be sent and attach it to the original message. Upon receiving the message, the receiving side applies the same hash function to the message and compares the resulting hash to the hash attached in the original message. Should the two hashes match, integrity is verified (i.e. it is proven that the message contents have not been altered in transit as a result of e.g. a message modification attack). Bhattarai et.al in [5], present their own lightweight digital watermarking technique as a simple, low-cost and efficient way to ensure defense against false data injection attacks. Digital watermarking is a technique of embedding digital data inside real time meter

readings, with the watermark carrying unique information about the owner of the reading. The purpose of the watermark is to validate the integrity of data. Watermarked data are sent from the meter to the utility through high speed unsecured networks that are prone to false data injection attacks. To ensure the successful detection of these attacks , the meters use low rate and secured channels to securely transmit the watermarks. The utility thus receives both the watermarks and the watermarked data, in order to correlate them and detect false data injection attacks Furthemore, Load Profiling, Timestamps, Sequence Numbers, etc are other techniques that can be used to ensure high integrity assurance. Fig 2 shows the various ways in which countermeasures .

Confidentiality and Privacy
▪ Symmetric/Asymmetric Encryption Algorithms (eg. AES/RSA/ECC) ▪ Anonymization ▪ Trusted Aggregators ▪ Homomorphic Encryption ▪ Perturbation Models ▪ Verifiable Computation Models – Zero Knowledge Proof Systems ▪ Data obfuscation
Integrity
▪ Cryptographic Hashing Techniques (eg. SHA-3) ▪ Digital Watermarking ▪ Adaptive Cumulative Sum Algorithm ▪ Installation of known secure PMUs in network ▪ Load Profiling ▪ Timestamps ▪ Sequence Numbers ▪ Session Keys ▪ Nonces
Authenticity
▪ Keyed cryptographic hash functions (eg. HMAC) ▪ Physically Unclonable Functions ▪ Hash based authentication codes ▪ MAC-attached and HORS-signed messages
Non Repudiation
▪ Mutual Inspection with Smart Meters ▪ Unique keys for customer-AMI communication ▪ AMI transaction logging
Availability
▪ Alternate Frequency Channels according to hardcoded sequence ▪ Frequency Quorum Rendezvous ▪ Anomaly Based IDSs ▪ Specification Based IDSs
Authorization
▪ Attribute Based Encryption ▪ Attribute Certificates ▪ Attribute Based Access Control System based on XACML

Figure 2: An overview of security counter measures by goal.[12]

4.6 Smart Home Security Systems

One major application of IOT in Homes is the power of monitoring the premises from anywhere. Smart security systems are highly customizable and available as do-it-yourself kits or as full-blown setups that include professional installation and monitoring. Therefore, customers have a choice in systems where they can either monitor the house themselves or can have it monitored by third parties on payment basis. There's also options in which one can have individual devices (like motion sensors, door locks, security cameras) rather than dedicated security systems which can be monitored via smartphones or tablets. As any general system would, the smart home security system can be connected to the Wi-Fi router of the house, giving access to customers remotely.

Ensuring Low Power Consumption :

In a perfect world, all home security components would use the same wireless standard to communicate with the main hub, but factors such as power requirements, signal range, price, and size make it virtually impossible to settle on just one. For example, smaller components such as door/window sensors typically use Z-Wave or Zigbee technology because they don't require a lot of power and can be powered by smaller batteries. They also operate in a mesh topology and can help extend the range of networked devices. However, neither protocol provides the bandwidth that you get with Wi-Fi, which is why it is usually used in security cameras to provide smooth video streaming, and in other devices that require a fat pipe. Moreover, Z-Wave and Zigbee devices are connected and controlled using a hub, while Wi-Fi devices can be connected directly to your home network and controlled with an app. Finally, Z-Wave and Zigbee devices use AES 128 encryption, and since they operate in a closed system with a dedicated hub, they offer more security than Wi-Fi devices.

A few Intelligent features :

With advancement in the intelligent IoT systems, more and more features are coming up. These features might be simple in nature but have a significant effect on the lives of people. For example, as soon as the smoke alarm goes off, all the doors should be unlocked. Or maybe the cameras could start recording as soon as a particular sensor goes off. Clearly, the first one will

help in saving lives in case of fires and the second will simply save up the memory usage, electricity usage, therefore, giving monetary advantages to the customer. All these with the advantage of easy modifications in the system using smartphones, give the users a lavish security system at a minimal cost. Another important feature to be noticed is the Video Doorbell which offers an easy way to see who is at your door without having to open or even get close to the door. These devices connect to your Wi-Fi network and will send an alert when someone approaches your doorway. They'll record video when the doorbell is pressed or when motion is detected, and usually offer two-way audio communication that allows you to speak with the visitor from anywhere via your phone. Another famous technology to be looked at here is, IFTTT. IFTTT derives its name from the programming conditional statement "if this, then that." What the company provides is a software platform that connects apps, devices and services from different developers in order to trigger one or more automations involving those apps, devices and services. This can allow the user to not necessarily go for a particular company for all the components needed in the system. The users as per their requirements can go for door locks, motion sensors, smoke detector systems of different companies and use IFTTT to bring them to a common platform. This especially comes in handy to people trying to install the system on their own. So,many companies also give the IFTTT support

5 Energy management solutions

Using energy efficiently in smart homes saves money, enhances sustainability and reduces carbon footprint at large. As a result, the need for smart energy management is on the rise for smart homes and for smart cities in general. However, the lack of low cost, easy to deploy, and low maintenance technology has somewhat limited a large-scale deployment of such systems. The sheer quantity of data collected throughout different cities of a country presents multiple challenges in data storage, organization, and analysis. Internet of Things (IoT) technology and Big Data are natural candidates to address these challenges. IoT technologies can provide a ubiquitous computing platform to sense, monitor and control the household appliances energy consumption on a large scale. This data is collected using many different wireless sensors installed in residential units. Similarly, Big Data technology can be utilized to collect and analyze large amounts of data [3]. Data

analytics on this data using business intelligence (BI) platform plays an essential role in energy management decisions for homeowners and the utility alike. The data can be monitored, collected and analyzed using predictive analysis and advanced methods to actionable information in the form of reports, graphs and charts. Thus, this analyzed data in real-time can aid home owners, utilities and utility eco-systems providers to gain significant insights on energy consumption of smart homes. The energy service providers can use the power consumption data available with analytics engine to provide flexible and on-demand supply with appropriate energy marketing strategies. The consumers, being aware of their consumption behavior and having a close interaction with the electricity utilities, can adjust and optimize their power consumption and reduce their electricity bills.

5.1 Energy Harvesting and Management

In order to have an effective cost saving system, it is important to monitor and control the operation of residential loads depending on the aggregate power consumption over desired period, the peak power consumption, the effect of weather/atmospheric conditions and consumption slab rates. This is where the combination of IoT technology, Big Data analytics and BI comes into play for implementing energy management solutions on a local and national scale. Finally, as an additional advantage, the use of IoT also enables seamless remote access control of home devices where the customers get online access to the ON/OFF usage pattern of in home appliances via a personal computer or a mobile phone.

Bharat et. al.[4] focused on the advantages of home automation such as - reduced installation cost, system stability, easy extension, aesthetically benefited and integration of mobile devices.

Farzana et. al. [18] in their research proposes an implementation of smart home automation system by dividing our regular household appliances into two categories, low load and some scheduled high load appliances. After automation and scheduling, a solar system power supply has also been incorporated that can supply power to some appliances and reduce power consumption from national grid. This system also provides a detail analysis on energy management which has been developed by measuring power consumption throughout a year in different seasons.

Another interesting approach by for implementing energy efficient automation is presented by Michael C. Mozer in [14], where they have devel-

oped a home system that essentially programs itself by observing the lifestyle and desires of the inhabitants, and learning to anticipate and accommodate their needs.The system controls basic residential comfort systems-air heating, lighting, ventilation, and water heating. They call the system ACHE. ACHE has two objectives.

- One is anticipation of inhabitants needs. Lighting, air temperature, and ventilation should be maintained to the inhabitants comfort; hot water should be available on demand. When inhabitants manually adjust environmental setpoints, it is an indication that their needs have not been satisfied and will serve as a training signal for ACHE. If ACHE can learn to anticipate needs, manual control of the environment will be avoided.

- The second objective of ACHE is energy conservation. Lights should be set to the minimum intensity required; hot water should be maintained at the minimum temperature needed to satisfy the demand; only rooms that are likely to be occupied in the near future should be heated; when several options exist to heat a room , the alternative minimizing expected energy consumption should be selected.

They archive the optimal control by defining an average energy cost function as

$$J(t_0) = \mathrm{E}\left[\lim_{\kappa\to\infty} \frac{1}{\kappa} \sum_{t=t_0+1}^{t_0+\kappa} d(x_t) + e(u_t)\right]$$

Where $J(t_0)$, is The expected average cost, starting at time t_0 , $d(x_t)$ is the discomfort cost associated with the environmental state x at time t, and $e(u_t)$ is the energy cost associated with the control decision u at time t

The goal is to find an optimal control policy (a mapping from x_t to decisions u_t) that minimises the expected average cost.

Il-Young Joo et. al. [11] proposes a distributed optimization algorithm for scheduling the energy consumption of multiple smart homes with distributed energy resources. In the proposed approach, the centralized optimization problem for home energy management is decomposed into a two-level optimization problem, corresponding to the local home energy management system (LHEMS) at the first level and the global home energy management system (GHEMS) at the second level. The controllable household appliances (e.g., air conditioner, washing machine) are scheduled in the LHEMS within

consumer's preferred appliance scheduling and comfort level while the energy storage system (ESS) and power trading between households are scheduled in the GHEMS. In the simulation study, the proposed distributed algorithm shows almost equivalent performance to the centralized algorithm in terms of the electricity cost and the consumer's comfort level. The impact of different network topologies on the proposed algorithm is also analyzed, and the result provides insight into the selection of the optimal network configuration in view of the consumer's electricity cost saving.

Junyon Kim et. al. [1] proposed a very simple and appropriate idea on smart home which includes internal home appliances and their internal connectivity. They called this model HEMS(Home Energy Management System) model using Internet of Things (IoT).

Zhao et al. [22] in their paper propose a smarter model on scheduling system that can be useful on our home automation system design assignment.

Haque et al. presented an optimized stand-alone green hybrid system to supply electricity in an island of Bangladesh called Saint Martin[9].

F Shabnam [17] talked about eco-friendly cellular network where base stations of cellular network will harvest energy and trade the excess harvested energy to electricity grids.

Various studies have been steered in the application of IoT environment for HVAC control and scheduling methods to optimize HVAC energy consumption [[16], [8], [19]]

5.2 Node energy management

Apart from papers that talk about using IoT to optimise power consumption and financial aspects of a house as a whole, techniques to minimise the IoT device power are discussed in the following paper.

The authors of [7] discuss a fuzzy logic based mechanism that determine the sleeping time of an IoT devices in a home automation environment based on BLE. The proposed FLC determines the sleeping time of field devices according to the battery level and to the ratio of Throughput to Workload (Th/Wl). Simulation results reveal that using the proposed approach the device lifetime is increased by 30% with respect to the use of fixed sleeping time.

5.3 Smart Grid Architecture

Various frameworks describing the architecture of a Smart Grid have been proposed, the most widely adopted and adapted model by far, being the reference model proposed by the U.S National Institute of Standards and Technology. [20]

Here the authors describe the the Smart Grid as a set of seven interconnected domains. The first four domains (Bulk Generation, Transmission, Distribution and Customers) are responsible for the generation, transmission and distribution of energy but also for ensuring the two way communication between the customer side and the Advanced Metering Infrastructure (AMI). The rest three entities (Markets, Operations and Service Providers) are inspired by NIST's conceptual model .

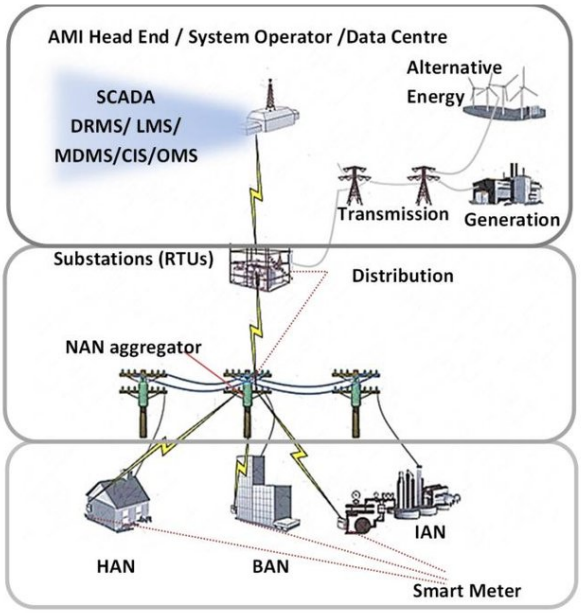

Figure 3: A multi-layered conceptual model of the Smart Grid's architecture. As described by NIST[12]

At the bottom layer of this model, one can find Home Area Networks (HANs), Building Area Networks (BANs) and Industrial Area Networks (IANs) i.e. wired or wireless networks in customer premises (homes, buildings or industrial areas) that interconnect appliances with smart meters and

energy management devices, responsible for reporting the premise's consumption to the grid at any given time while also carrying messages from the grid back to the premise. Komninos et. al [12] breifly cover this Smart Grid Architecture in their paper.

5.4 Communication

A HEMS requires a reliable communication network using WSN that can transport the consumption details and consumer load behavior periodically. In [[2], [15], [6]], an implementation of a HEMS Unit in a Wireless Sensor Network using a ZigBee Module to communicate with sensor nodes, is presented. The system monitors the device consumption data and sends control signals to end nodes during peak load hours. However, the lifetime of a WSN network deteriorates with time due to the deployment of new sensors in the network. Additionally, Han et al. in [10] introduced a system for monitoring power consumption using ZigBee as the communication protocol in a WSN. However, in this system the data was collected and aggregated solely by the home server which could lead to data loss in case of a system failure. Moreover, a bridge between ZigBee and TCP/IP stack would be required to connect this system to a community of homes. The above mentioned WSN networks have been extended to wider ranges in the IoT paradigm utilizing the GSM/GPRS networks to remotely control the end-devices in [[21], [13]].

6 Voice assistance

7 Challenges of Home automation systems

8 Conclusion

References

[1] Hems (home energy management system) base on the iot smart home. *Contemporary Engineering Sciences*, 9:21–28, January 2016.

[2] M. Abo-Zahhad, S. M. Ahmed, M. Farrag, M. F. A. Ahmed, and A. Ali. Design and implementation of building energy monitoring and manage-

ment system based on wireless sensor networks. In *2015 Tenth International Conference on Computer Engineering Systems (ICCES)*, pages 230–233, 2015.

[3] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar. A smart home energy management system using iot and big data analytics approach. *IEEE Transactions on Consumer Electronics*, 63(4):426–434, 2017.

[4] S. Bharath and M.Y. Pasha. Iot-home automation. . *International Journal of Computer Technology and Research*, 5:4–6, April 2017.

[5] S. Bhattarai, L. Ge, and W. Yu. A novel architecture against false data injection attacks in smart grid. In *2012 IEEE International Conference on Communications (ICC)*, pages 907–911, 2012.

[6] J. Byun, I. Hong, B. Kang, and S. Park. Implementation of an adaptive intelligent home energy management system using a wireless ad-hoc and sensor network in pervasive environments. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6, 2011.

[7] M. Collotta and G. Pau. Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes. *Computers & Electrical Engineering*, 44:137–152, 2015.

[8] K.F. Fong, V.I. Hanby, and T.T. Chow. Hvac system optimization for energy management by evolutionary programming. *Energy and Buildings*, 38(3):220–231, 2006.

[9] K. Foysal Haque, N. Saqib, and M. S. Rahman. An optimized standalone green hybrid grid system for an offshore island, saint martin, bangladesh. In *2019 International Conference on Energy and Power Engineering (ICEPE)*, pages 1–5, 2019.

[10] J. Han, C. Choi, W. Park, I. Lee, and S. Kim. Smart home energy management system including renewable energy based on zigbee and plc. *IEEE Transactions on Consumer Electronics*, 60(2):198–202, 2014.

[11] I. Joo and D. Choi. Distributed optimization framework for energy management of multiple smart homes with distributed energy resources. *IEEE Access*, 5:15551–15560, 2017.

[12] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys Tutorials*, 16(4):1933–1954, 2014.

[13] G. Mingming, S. Liangshan, H. Xiaowei, and S. Qingwei. The system of wireless smart house based on gsm and zigbee. In *2010 International Conference on Intelligent Computation Technology and Automation*, volume 3, pages 1017–1020, 2010.

[14] M. Mozer. The neural network house: An environment that adapts to its inhabitants. 1998.

[15] N. Nguyen, Q. Tran, J. Leger, and T. Vuong. A real-time control using wireless sensor network for intelligent energy management system in buildings. In *2010 IEEE Workshop on Environmental Energy and Structural Monitoring Systems*, pages 87–92, 2010.

[16] Jordi Serra, David Pubill, Angelos Antonopoulos, and Christos Verikoukis. Smart hvac control in iot: Energy consumption minimization with user comfort constraints. *The Scientific World Journal*, 2014:161874, Jun 2014.

[17] F. Shabnam. Analysis of energy harvesting techniques for mobile networks. In *2019 IEEE Region 10 Symposium (TENSYMP)*, pages 784–788, 2019.

[18] F. Shabnam, T. U. Islam, S. Saha, and H. Ishraque. Iot based smart home automation and demand based optimum energy harvesting and management technique. In *2020 IEEE Region 10 Symposium (TENSYMP)*, pages 1800–1803, 2020.

[19] Tacklim Lee, Seonki Jeon, Dongjun Kang, Lee Won Park, and Sehyun Park. Design and implementation of intelligent hvac system based on iot and bigdata platform. In *2017 IEEE International Conference on Consumer Electronics (ICCE)*, pages 398–399, 2017.

[20] National Institute of Standards and Technology U.S. Department of Commerce. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 [Online] Available : http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.*

[21] J. Wang, J. Huang, W. Chen, J. Liu, and D. Xu. Design of iot-based energy efficiency management system for building ceramics production line. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, pages 912–917, 2016.

[22] Zhuang Zhao, Won Cheol Lee, Yoan Shin, and Kyung-Bin Song. An optimal power scheduling method applied in home energy management system based on demand response. *ETRI Journal*, 35(4):677–686, 2013.