SURE-H: A Secure IoT Enabled Smart Home System

Roshmi Sarmah
Department of Information Technology
Sikkim Manipal Institute of Technology
Majitar, Sikkim 737132, India
*reshmisharma*01@*gmail.com*

Manasjyoti Bhuyan
DEIB-Computer Science and Engg.
Politecnico di Milano
Milan 20133, Italy
bhuyanmj@gmail.com

Monowar H. Bhuyan†
Department of Computing Science
Umeå University
Umeå-901 87, Sweden
monowarb@ieee.org

***Abstract*—With the growing technology, the demand for smart things is drastically increased in daily-life. The IoT (Internet of Things) is one of the major components that provides facility to interact with IoT enabled devices. In this work, we propose a secure and efficient smart home system that enable to protect homes from theft or unusual activities and parallelly saves power. Our system is developed by exploiting the features of IoT that facilitates us to monitor an IoT enabled home from anywhere anytime over the Internet when data are stored in the cloud. This system uses a motion detector to detect a moving object from the environment where the system is deployed. The proposed system is evaluated using real-time deployment at KU campus considering 30 rooms for 60 days and found really useful in terms of safeness from any theft and saving power in comparison to existing systems.**

***Index Terms*—IoT; smart home; android smart phone; home automation; motion sensor;**

I. Introduction

With proliferation and uses of Internet technology, the demand for IoT enabled devices has increased explosively. At the same time, there are problems regarding burglary or theft anything from small houses to large industries. Constant monitoring of people's behavior, activities are required for the purpose of protection and management of confidential data [1], [2]. In surveillance, installing and setup of CCTV camera systems becomes costly for normal residents and also system can not inform the owner's automatically when the robbery happens. Compared to existing systems [3], [4], the ESP8266 system is better in terms of resolution and low power consumption. Here, passive infrared (PIR) sensors are used as a simple but powerful people presence triggers. This system is suitable for small personal area monitoring like personal office cabin, bank locker room, parking entrance, and home. Whenever motion is detected through a PIR sensor which is fitted with the ESP8266 module, information is stored temporarily in that module. The various IoT-based application can be used remotely to monitor the activity and receive notifications when motion is detected. Once programmed, the system works as a stand-alone. An Android application is developed for home owners to accept various notifications when the system detects any moving object.

Machine to Machine (M2M) interaction is a new business concept originating from the telemetry technology used for automatic transmission and measurement of data from remote sources by wire, radio or other means [5]. The use of M2M communication is more beneficial than a traditional system with human intervention. As the system becomes automated and flexible to upgrade, it becomes cheap to develop and cost-effective to operate thereby increases the efficiency of the system drastically.

In this work, we present a secure IoT-enabled smart home system that increases safeness from theft and parallelly saves enormous power cost. We deploy each configured module at KU campus for 30 rooms to evaluate the performance of the proposed system and found effective in terms safeness as well as power cost. It uses an Android application which provides switching functionalities, where the electrical or electronic devices are monitored and controlled remotely. This system adds advantage by eliminating the use of traditional personal computers (PC) and its peripheral devices during execution.

The rest of the paper is organized as follows: this work focuses on the security control and saves the power of smart home automation system. We first discuss related literature in Section II on smart home automation system followed by our proposed system and its implementation in Section III. Experimental results are reported in Section IV. Finally, we present conclusions in Section V followed by future work.

II. Literature Review

Back in the 1980s, Japan, US and Europe had taken the initiatives to develop more comprehensive home automation systems. The term home automation system was first used by the Japanese companies like Hitachi and Matsushita who showed the interest in home automation systems. The Smart House Project was established in 1984 as project of the National Research Center of the National Association of Home Builders (NAHB), USA, with the cooperation of a number of major industrial partners [6]. NAHB formed the SMART HOUSE Limited Partnership. It is comprised of major manufacturer companies and provided supports for the hardware and software required for the home automation system [7].

†Dr. Bhuyan is on lien from the Department of Computer Science and Engineering, Kaziranga University, Jorhat 785006, Assam, India since September 2017.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

Alkar and Buhur [8] implement Internet-based wireless solution to connect home devices to a slave node. The slave nodes communicate with a central node through radio frequency and master node had serial RS232 link with a PC server. The PC server includes a user interface component, a database and web server components. An Internet page had been setup and running on a Web server. The control of devices is established and their condition is monitored through the Internet. The test results showed that the wireless communication has limited range less than 100 meters in concrete building. Yavuz *et al.* [9] design and implement a telephone and PIC (programmable interface) remote controlled device for controlling the home electrical devices. The system does not facilitate wireless communication rather it uses pin check algorithm to work with cable networks. The system ensured safety as it cannot be used by unauthorized users as the system uses pin-check system.

Das *et al.* [10] present a GSM-based communication and control for home appliances. This system allows the user or home owner to monitor and control the home appliances via mobile phone set by sending commands in the form of SMS (short message service) messages and the system also provides current status of the home appliances. They used wireless control, hence, the system can be effectively used in systems not connected through wire which was desired in that moment. The working principle was user send text message through the GSM network. GSM received the message send it to the ATMEGA8 microcontroller via serial port using internal UART [11] module of ATMEGA8. A microcontroller keeps polling to check if the modem has received any text message. ATMEGA8 communicates through a special command set known as "AT COMMAND SET". The microcontroller decodes action required corresponding to the SMS command by a search and match technique where a look-up table is created with a set of commands and corresponding actions. Tseng *et al.* [12] present a Smart House Monitor and Manager (SHMM) based on ZigBee, all sensors and actuators are connected by a ZigBee wireless network. They designed a simple smart socket, which had remote control via ZigBee. A PC host is used as a data collector and for motion sensing, all sensor data are transferred to the Virtual Machine (VM) in the cloud. The user can use a PC or Android phone to monitor and control through the Internet to perform power-saving of the house.

A. Discussion

As we entered into the 21st century, the interaction between humans and computer is breaking old barriers and entering a new realm. In the highly technology driven world, the mobile phones have become a part of our lifestyles. Mobile phones are not just communication tool, it is much more than that. Our work tries to derive solution providing better security system for the home or office along with smart control on home appliances with the help of cell phone. The existing system consists of the manual security system that raise alarm on breakthrough which can be heard to a limit of a particular range about 50 meter. But what if the owner is not at home? How can he monitor his house or office remotely? Moreover, this system is less secured and prone to electrical hazards. This prototype provides a solution to this problem and enables energy saving as well. To support and introduce a cost effective solution, the attempted system is pertaining to connect multiple home appliances via smart logic circuit. This system adds benefits to the traditional residents to monitor, control home appliances, and parallelly save power from anywhere and anytime through smartphone applications.

III. SURE-H: The Proposed System

The proposed automated smart home system consists of three main modules such as (i) the cloud server, (ii) the hardware interface module, and (iii) the software package or smartphone application.

To design SURE-H system, initially, the sensors are configured and attached to the ESP8266-12E module. This module is capable to accept instruction through an interfacing port. The ESP8266-12E module of the relay board is programmed with Arduino and then it is configured to receive and process a specific command transmitted over the Internet from user. The cloud server is configured based on a cloud service provider known as Blynk. Blynk provides end-to-end solution for IoT based application development. Finally, we design a smartphone app and connected with the ESP8266-12E module through a cloud service provider over the Internet.

Figure 1 shows the prototype model of the proposed system. User uses the Internet to login into the cloud server and control the home automation system. Low voltage switching relays are used to integrate devices with the ESP8266-12E module for demonstrating the switching functionality. If server is connected to the Internet then remote users can access server using web-based application over the Internet.

SURE-H come up with following features.

- automated switches for all home appliances
- capable to detect moving object
- generate password by combining user password and fingerprint

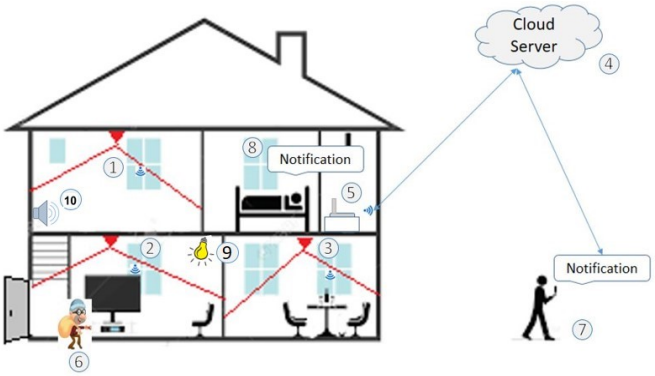
The SURE-H system works based on the stored cloud server data. We store the details of home appliances for each room into the server. Initially, it sends a request to the server and wait for the approval. As soon as it observes any motion object it sends an alarm with detail report against the incident. This alarm will trigger only when the new object observes. Figure 2 shows the flow of data of the SURE-H system.

A. SURE-H: The Proposed Algorithm

As SURE-H operates through an Android app, it controls the automated home system efficiently. Algorithm 1 demonstrates the major steps of the SURE-H system.

IV. Experimental Results

In this section, we present experimental results with parameter estimation. Parameter estimation is really necessary to fit the system in real-time environment.



1) Motion detector PIR sensor
2) Motion detector PIR sensor
3) Motion detector PIR sensor
4) Blynk cloud server
5) WiFi Internet gateway
6) Thief
7) User 1 getting notification
8) User 2 getting notification
9) Lights automatically turns on detection of the thief
10) An alarm is also raise on detection of the thief

Fig. 1. SURE-H: a prototype model of autonomous smart home system

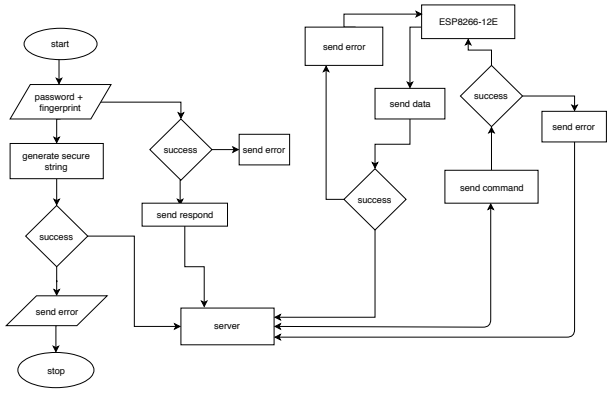


Fig. 2. SURE-H: a dataflow diagram

A. Experimental setup

To evaluate a system in real-time, it is really important to deploy the system in real environment. We setup and deploy modules in 30 different rooms for 60 days to observe the efficiency, which is designed based on an approximation model of power consumption for each room. During the period, we measure the efficiency of detection theft and power cost per room after each five alternative days. To estimate the total cost, we compute (i) the total hours consumes the power, $t_h = (consumed\ time\ in\ seconds/60\ seconds) \times (24\ hours/day)$, (ii) the total hours in a months, $t_m = (t_h \times number\ of\ days)$, (iii) the total watts consumed, $t_w = t_m \times \%\ of\ total\ watts\ bulbs\ or\ devices\ deployed$, (iv) the total cost, $T_c = t_w \times rate\ per\ unit$. SURE-H system follows two major steps to accomplish this task.

Algorithm 1 SURE-H(S, UID, PASS)

Input: Power supply to the IoT enabled devices (S), user ID of the house owner (UID), password for the particular user(PASS) and fingerprint (F).

Output: Control IoT enabled devices and automatic object detection.

1: Initialize the app and ESP8266-12E module.
2: App and ESP8266-12E module is configured with a remote server (blynk server).
3: Send the data to the server and server send it to ESP8266-12E module.
4: ESP8266-12E processes the data and send back the data through the remote server.
5: Blynk server send the data to the app on request and displayed on app
6: Compare the received string with predefined strings and accordingly activate the sensors and switch the Electrical loads.
7: Display the status of electrical loads on app.
8: Exit

Step 1: Setting up ESP8266-12E relay board

After getting ESP8266-12E board, we write instructions that passes through Arduino. After that required relay board was connected to the GPIO pins and power cable with 220v-240v AC connection. The various home appliances are connected to the Solid State Relay (SSR) switches. The AC is converted to DC with the help of AC to DC converter to pass current to the board.

Step 2: Operating ESP8266-12E with smartphone

ESP8266-12E is attached with Internet through Wi-Fi or any other connectivity so that it can be accessed through cloud server. Through Arduino IDE ESP8266-12E, it is programmed and works in stand-alone mode. An Android or iOS application is installed in the user's smartphone which can connect to the same cloud server through either IP address of the server or domain name. Moreover, user should provide the password and fingerprint to login to the server. Finally, the user can monitor their home or office remotely from anywhere and anytime with low cost and save power consumption.

B. Results and discussion

The Arduino script monitors the difference in IR (infrared) signal of the motion sensor, if there is any interference in IR signals then the motion flag is set, triggering the buzzer and switching on the light. When the motion is detected, sensor data will trigger out and it will send a notification to Android or iOS application installed in the user's smartphone and connected email account. It will then report any intrusion inside the surveillance area and make the user aware of the situation in every 5 second. Figure 3 demonstrates the app activity for a single room.

The smart home system was fully functional and the user interface is updated to reflect the current status when the appliances are switched on. The SURE-H system is tested

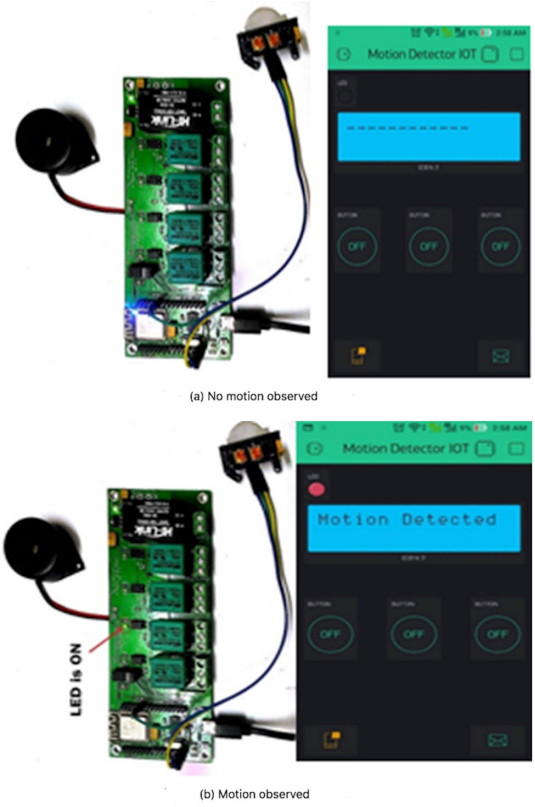


Fig. 3. SURE-H android app

for intrusion whereby it successfully detects the respective events generating an email to the user and turning on the buzzer. It has security features such as user authentication for accessing the SURE-H system, and intrusion detection with alert notification. The system does not require a dedicated PC that makes it low-cost and affordable. At the end, we estimate the power consumption cost at each alternative five days before and after deployment of the proposed system.

To work in high-speed networks, SURE-H performs well in terms of time, cost, security and low infrastructures than [3], [9], [13], [14]. Frequency range of existing systems are $900 - 928$ MHz and 2.4 GHz, and network range is $10 - 30$ meters. SURE-H works in frequency range 2.4GHz and 5GHz, and network range is between 30 to 100 meters. In fact, we save power consumption cost as seen in the Figure 4. Hence, it is clear that SURE-H outperforms existing systems.

C. Security and vulnerability analysis

SURE-H is developed to protect smart home system. Like other systems, SURE-H is also vulnerable to two major attacks: (i) man-in-the-middle attack (ii) online dictionary attack. Each of them explained below briefly.

- *Man-in-the-middle attack*: In this attack, an adversary attempt to impersonate the communication between the server and the app. We provide additional layer of security by combining classical password and fingerprint [15] to generate the actual password.

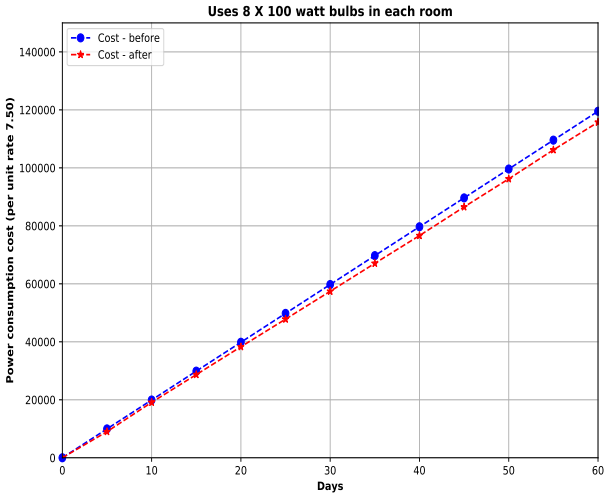


Fig. 4. Power consumption cost for 60 days in 30 deployed rooms

- *Online dictionary attack*: This attack is commonly attempt to guess the password during communication between the parties either system or human. We generate 256-bits password using one-way hash before sending for verification. Hence, it resist this attack.

V. Conclusion and Future Works

In this paper, SURE-H system is presented to ensure security of smart home automation system with multiple components such as users, motion sensors, cloud server, moving object detection module, and alarm module. It is controlled remotely based on user authentication. The SURE-H system has been designed in such a way that it can fullfil the needs of the user that reduces manual effort, save power and makes more secure. Any android device can be used to monitor the smart home environment to detect any robbery. It has several features include low cost, minimum time, highly scalable, resist against man-in-the-middle and online dictionary attacks, and needs minimum infrastructures.

SURE-H can be extended to the large-scale environment such as offices and companies. It can also add additional features such incorporating camera, call alerts and live video streaming for future reference and analysis.

Acknowledgment

This work was carried out when the authors attached with the Department of Computer Science and Engineering, Kaziranga University, Jorhat 785006, Assam, India and supported by the Kempe post-doc fellowship with the project no. SMK-1644.

References

[1] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, *Network Traffic Anomaly Detection and Prevention - Concepts, Techniques, and Tools*, 1st ed., ser. Computer Communications and Networks Series. Springer International Germany, 2017.

[2] D. Choi, S. Seo, Y. Oh, and Y. Kang, "Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 335–348, Feb 2019.
[3] N. Sriskanthan and T. Karand, "Bluetooth based home automation system," *Journal of Microprocessors and Microsystems*, vol. 26, pp. 281–289, 2002.
[4] R. Petrolo, V. Loscri, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, pp. 1–12, 2015.
[5] S. Joshi, A. Joshi, S. Jabade, and A. Jathar, "M2M Communication Based Wireless SCADA for Real-Time Industrial Automation," *International Journal of Research in Advent Technology*, vol. 2, no. 4, pp. 107–109, 2014.
[6] M. Kumar and R. Singh, "Home appliance controlling using zigbee on atmega128 hardware platform," *International Journal of Research in Engineering and Technology*, vol. 3, no. 7, pp. 469–472, 2014.
[7] A. C. Jose and R. Malekian, "Smart home automation security: A literature review," *Smart Computing Review*, vol. 5, no. 4, pp. 269–285, 2015.
[8] A. Z. Alkar and U. Buhur, "An internet based wireless home automation system for multifunctional devices," *IEEE Transactions on Consumer Electronics*, vol. 51, pp. 1169–1174, 2005.
[9] E. Yavuz, B. Hasan, I. Serkan, and K. Duygu, "Safe and secure pic based remote control application for intelligent home," *International Journal of Computer Science and Network Security*, vol. 7, no. 5, 2007.
[10] S. Das, N. Debabhuti, R. Das, S. Dutta, and A. Ghosh, "Embedded system for home automation using sms," in *IEEE International Conference on Automation, Control, Energy and Systems*, 2014, pp. 1–6.
[11] S. Kumar, "Ubiquitous smart home system using android application," *International Journal of Computer Networks & Communications*, vol. 6, no. 1, 2014.
[12] S. P. Tseng, B. R. Li, J. L. Pan, and C. Lin, "An application of internet of things with motion sensing on smart house," in *IEEE International Conference on Orange Technologies*, 2014, pp. 65–68.
[13] V. M. Reddy, N. Vinay, T. Pokharna, and S. S. K. Jha, "Internet of things enabled smart switch," in *13th International Conference on Wireless and Optical Communications Networks*, 2016, pp. 1–4.
[14] M. Mongiello, F. Nocera, A. Parchitelli, L. Patrono, P. Rametta, L. Riccardi, and I. Sergi, "A Smart IoT-Aware System For Crisis Scenario Management," *Journal of Communication Software and Systems*, pp. 91–98, 2018.
[15] M. H. Bhuyan and D. K. Bhattacharyya, "An Effective Fingerprint Classification and Search Method," *International Journal of Computer Science and Network Security*, vol. 9, no. 11, pp. 39–48, 2009.