A Cyber-Secured MQTT based Offline Automation System

Nahian Ibn Hasan[1], Md. Tasnimul Hasan[2], Nazmul Haque Turja[3], Rishad Raiyan[4], Shuvagata Saha[5], and Md. Farhad Hossain[6]

[1,2,3,4,5,6]Department of Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology, Dhaka, Bangladesh
[1]nahianhasan1994@gmail.com, [2]muhammadtasnimulhasan@gmail.com, [3]nht570@gmail.com, [4]sa.dip987@gmail.com, [5]amidipu8@gmail.com, [6]mfarhadhossain@eee.buet.ac.bd

***Abstract*—In the era of digitization and computer information, cyber-attacks have been increasing on the IoT devices all over the world. Additionally, web-based IoT dashboards are costly. Since data exchange through the Internet is a must for almost every system, a sudden interruption in the Internet may disrupt or crash the system immediately. This paper presents a new cyber-secured MQTT based offline system addressing all the above issues that can automate various systems (e.g., super stores, ware houses, buildings and factories) integrated into a single dashboard where monitoring and controlling can be simultaneously executed.**

***Index Terms*—MQTT, cyber-secured, automation, IoT, Raspberry-Pi, ESP8266, Python, OpenCV.**

I. Introduction

Internet of things (IoT) is a concept which allows the devices to communicate over the Internet. The number of IoT devices are increasing at a brisk rate every year. CISCO IBSG predicts that the number of IoT devices will be about 50 billion by the year of 2020 [1]. IoT devices comprise of sensors, actuators, refrigerators [2], health trackers [3], smart home automation systems [4], automated irrigation systems [5] and others. Low power consumption, low data usage, etc. are the main hallmarks for IoT devices.

Many protocols are used in the IoT devices, such as Constrained Application Protocol (CoAP), Hypertext Transfer Protocol (HTTP), Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP) and Message Queue Telemetry Transport (MQTT) protocol [6]. Among them, MQTT is considered to be the most widely adopted connection protocol, standardized by ISO (ISO/IEC 20922: 2016) for machine to machine (M2M) and IoT. MQTT is very reliable as it has the ability to secure multicast message and also has some advanced functionalities (e.g., exactly once delivery, message persistence, etc.) [7]. It uses less amount of data and consumes less battery power. MQTT generally works on default TCP/IP with port 1883 [8]. It is standardized by OASIS Technical Committee. This protocol is very easy to work with and also provides Quality of Services (QoS) to the network with the minimum network bandwidth [9]. In MQTT, publishers and subscribers exchange messages through a centralized broker using MQTT control packets. The publishers generate data and publish that data to the message broker. In order to receive the message from the publishers, the subscribers need to subscribe based on the topic of interest [10]. At the present time a large number of security threats are happening in the field of IoT. A report which was released by L3 communications in 2016 suggests that some bots had infected about one million devices and were hosted in Colombia, Brazil and Taiwan [11]. Moreover, a Distributed Denial of Service (DDoS) attack had been made to krebsonsecurity.com site. It was performed by botnets, which were embedded in the IoT devices.

As the IoT attacks have increased and the security of the IoT devices are also being challenged, this paper proposes an application specific secured framework. More specifically, we propose a secured scheme for offline monitoring and controlling of ACs, chillers and refrigerators in a superstore using the MQTT server-broker-client system.

In this paper, section II describes our proposed system model along with the MQTT server, sensors used to obtain the real time data, AC control mechanism using an analytical model. Section III represents the system analysis using the commercially compatible software.

II. Proposed System Model

In our proposed system, we develop a control mechanism for the equipment taking temperature, humidity and human occupancy into consideration. The system is then implemented in hardware and its performance for a real superstore has been analyzed. In the proposed system, monitoring and controlling of the ACs, chillers and refrigerators can be executed over a short range of area through a router. As this intra-net system is offline and can be monitored within the router range, the cyber-attacks can't occur via the Internet. Fig. 1 illustrates the overall system infrastructure.

A. MQTT server

Proposed system depends on an MQTT server for communicating between the various systems components. Any device connected to the server can publish a message with a specific tag called a topic. The server listens for these messages and once it receives them, dispatches it to every device subscribed to that specific topic. The communication

978-1-5386-9279-0/19/$31.00

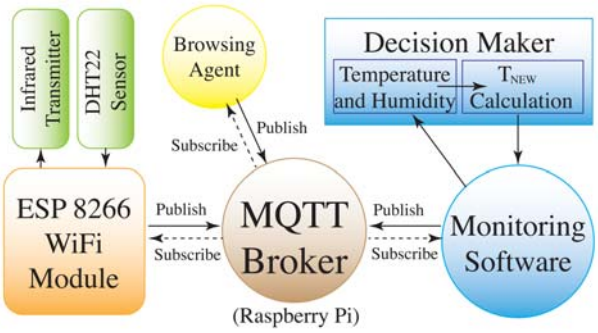


Fig. 1. Overall architecture of the proposed system.

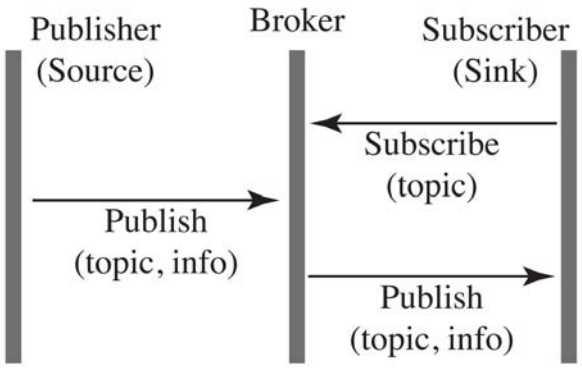


Fig. 2. Publishing, subscribing and processing in MQTT.

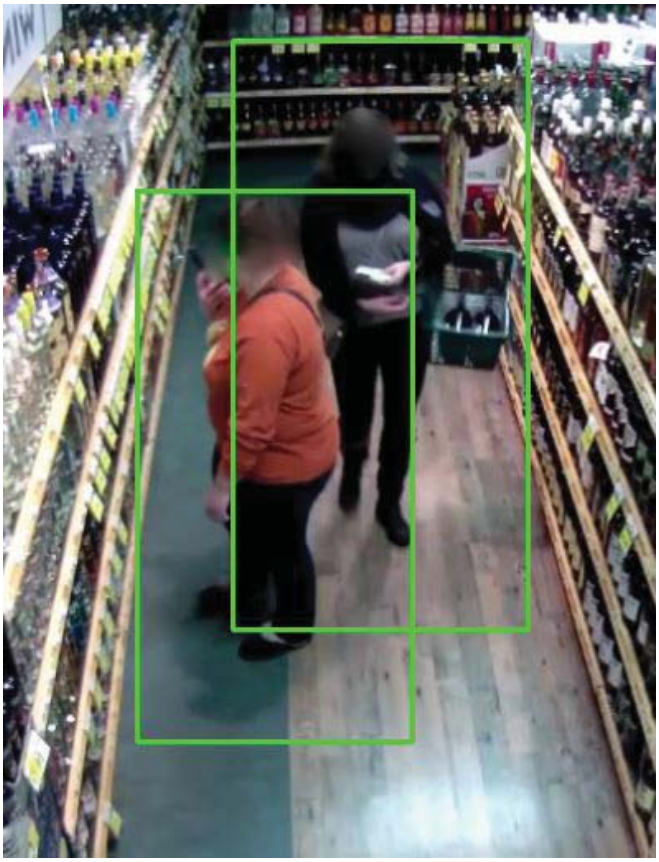


Fig. 3. Illustration of detecting humans and counting in real-time CCTV footage.

is illustrated in Fig. 2. Each IoT device uses a hierarchical naming scheme for topics while communicating to maintain clarity and extensibility.

The MQTT server is hosted inside a Raspberry-Pi using Eclipse Mosquitto, an open source message broker service. Every IoT device then connects to this central server using its IP address and port number. To assist this process, a special protocol called Multicast DNS (mDNS) is used. MDNS can assign a friendly name against any device connected to the network. The name can be used to look-up an IP address and port number. The devices with the associated names can broadcast their current IP address and port number, which are then stored in a table of the MQTT server for future look-ups. This way any new device can be added to the system without worrying about its IP address.

B. Temperature and Humidity Sensor

Our system also includes a set of ESP8266s with a DHT22 temperature and humidity sensor, which periodically sends data to the central server to monitor different parts of the superstore for comfort levels. The corresponding data is then used to create a heat map overlaid on top of a schematic of the building.

C. Human Counter

The software retrieves data from the CCTV footage camera. Then using image processing and analysis, it determines the human occupancy. Hence, the manual operation of the system is done with the help of this data. Moreover, people can be tracked present in the arena and shown in the software interface.

To compute number of people in a row of a superstore from CCTV footage, computer vision techniques (OpenCV) are used. Due to various possibility of poses and appearances, detecting humans in an image by computer is a difficult task. There are various techniques to detect human from an image. In this work, locally normalized HOG (Histogram Oriented Gradient) descriptors are used. This process evaluates locally normalized histogram gradient. Firstly, the input image is normalized. There are several blocks which are arranged in an overlapping grid manner. This arrangement extracts HOG features. The feature vectors are then combined to feed a state vector machine (SVM). This linear SVM classifies the image for human or non-human detection. In Fig. 3, a sample frame of person detection is shown (the persons' faces are blurred out manually after detection for privacy concerns).

D. Proposed T_{new} Calculation for AC

Temperature control is automated using the ISO 7730 [12] standard for analytical determination of PMV and PPD indices and local thermal comfort criteria which gives a mathematical equation for Predictive Mean Vote (PMV). PMV determines the comfort temperature for a room using a large number of

votes from people. PMV is a seven-point thermal sensation scale with values between −3 to +3 with 0 meaning the most comfortable. Positive PMV stands for hot sensation and negative PMV stands for cold. Calculation of PMV takes many factors into account. For this specific system, we assumed all the parameters as constant except for ambient temperature, humidity and presence of people. The corresponding data for these three parameters are fed to the system using the sensors mounted at different parts of the shopping mall. The metabolic rate for each person is taken as $93W/m^2$ or 1.6 Met [13] assuming shoppers standing or doing light activity. The wind velocity is taken as 0.1 m/s and basic clothing insulation is taken as 1 clo or $0.155W/m^2K$. When there are no people present, the corresponding AC temperature is defaulted to 25°C in an area. Otherwise the new temperature is calculated using equation 1, rounded off and the corresponding AC temperature is updated accordingly. Equation 1 improves the PMV so that the absolute value of the new PMV stays below 0.5.

$$T_{new} = T_{current} - 4 * PMV \tag{1}$$

E. Implemented AC Control System

The Air-conditioners (AC) are controlled by Infrared pulses driven by a NODEMCU ESP8266 which in turn connects wirelessly with the MQTT servers via Wi-Fi. These infrared signals are generated using a Pulse Width Modulation (PWM) pin on the ESP8266 connected to an infrared LED via a BJT. The BJT ensures proper amount of current flow through the LED, which in turn determines its range. Circuit diagram for the operation of the infrared LED is shown in Fig. 4. The PWM pin which transmits the signal is connected to the base of the BJT. The infrared LED can be powered using a battery with a current limiting resistance for even higher range as long as the LED is not burnt out as sometimes the maximum available current from the ESP8266 microprocessor may not be high enough.

Each AC manufacturer has different signaling conventions for each of the settable temperatures and on/off commands. The signals from different companies vary in bit-length, pulse width, frequency and interval between corresponding signals

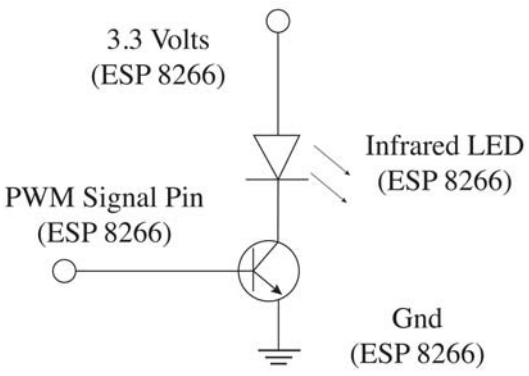


Fig. 4. Circuit for infrared LED operation to control AC.

[14]. We have made a special trainer module with an IR receiver that can read infrared signal from AC remotes in real time and pass it on to a software wirelessly. Inside the graphical user interface, we can associate the infrared codes with their associated commands. Afterwards, infrared signals and their corresponding commands can be stored inside the RaspberryPi for use. This trainer module is also equipped to detect the manufacturer and the number of bits in the signal. Both of these will be necessary later on to reproduce the signal.

In order to decode the IR transmission signals to acquire the related information, a special ESP8266 library was used [15]. The same library also has built-in functions to reproduce those signals using an infrared LED. Before setting up a system, we need to use the trainer module for each AC. The trainer module is required to store the codes for on/off commands as well as the codes for each of the temperatures available for the AC, conventionally from 18°C to 30°C. Otherwise the system will not function.

III. System Analysis

The real-time monitoring and controlling of the whole system is performed through a software from the operator station of the arena. The monitoring parameters include the temperature of chillers, refrigerators and air conditioners (AC); humidity, number of people in the arena, etc. The system is controlled automatically through temperature and humidity sensors, heat-maps from the CCTV footage and analyzing the number of people. Besides, there are user friendly provisions for manual control by the operator in case of emergency. This section explores the interface of the software and hardware stations and also the numerous aspects of the software.

A. Overall Interface of the Software and Hardware

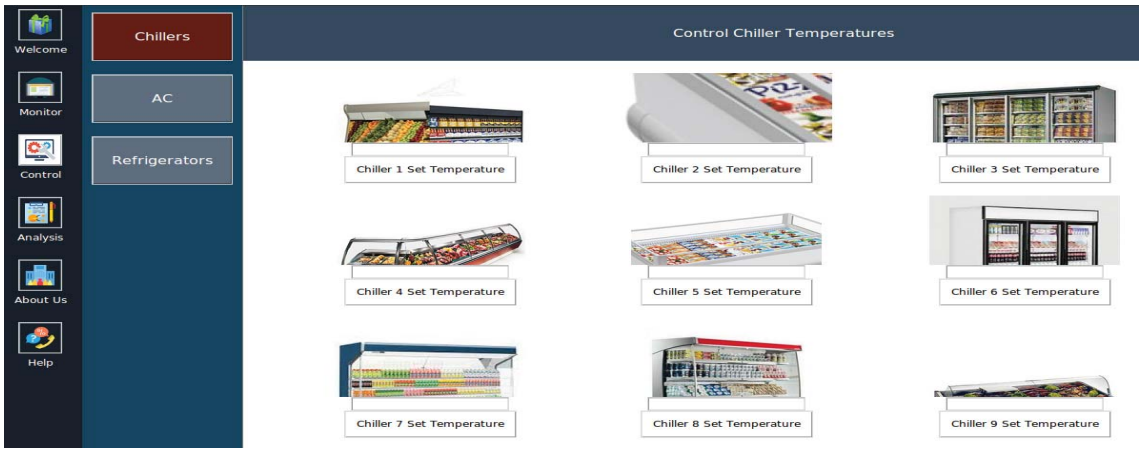
Data exchange between the hardware and software is performed through MQTT protocol. In this case, the Raspberry-Pi is acting as a broker between the Raspberry-Pi web server and the software client. When any controlling signal is published through the broker, that signal is available to the respective hardware station. Similarly, the monitoring data from the hardware stations are published through the web server and available to the software.

B. Manual Control

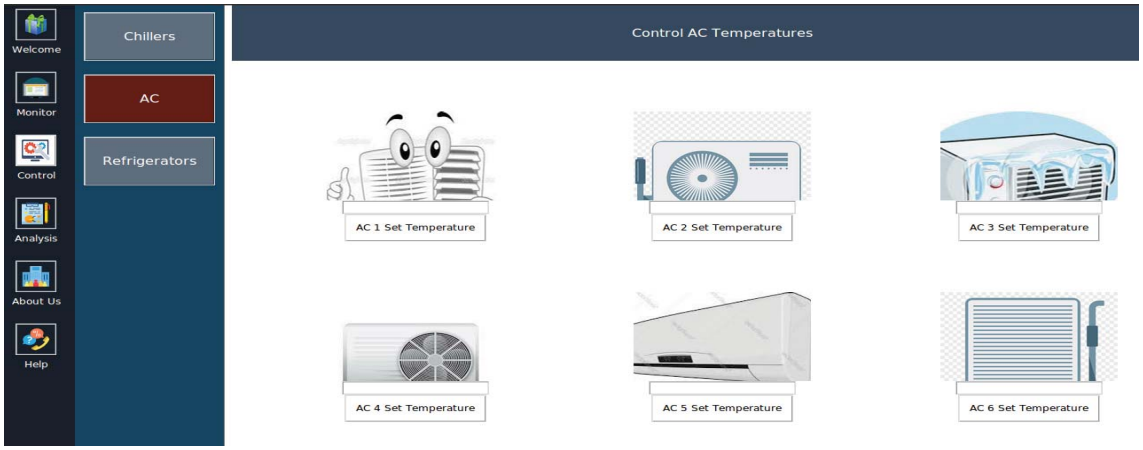
If the system fails to retrieve data or take decision in an automatic manner, the operator can change the system parameters manually from the software station. There are provisions for every hardware control from the software. Fig. 5 shows the features, where individual category of hardware can be controlled separately by the operator.

C. Heat-map

The overall temperature of the area can be shown as the heat-map in real-time in the software. The sample heat map of the area at a specific time is illustrated in Fig. 6. This helps the operator to control the temperature manually and monitor a particular area.



(a)



(b)

Fig. 5. Manual control interface for (a) chillers and (b) ACs in the software. Each category of appliances can be controlled separately. Besides individual appliances can be controlled from the software interface.

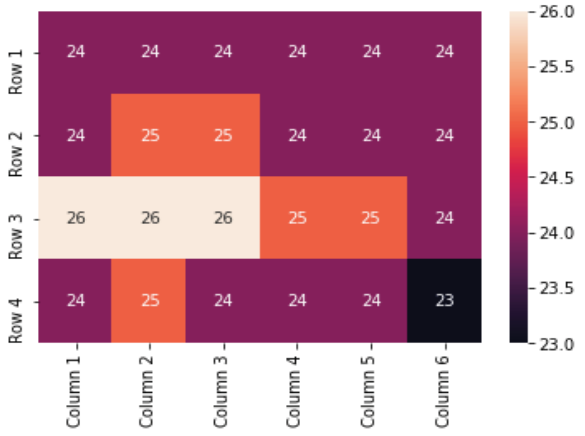


Fig. 6. Software visualization of heat map generated from data gathered from the temperature sensors installed around the store at a certain time.

D. Monitor and Automatic Control

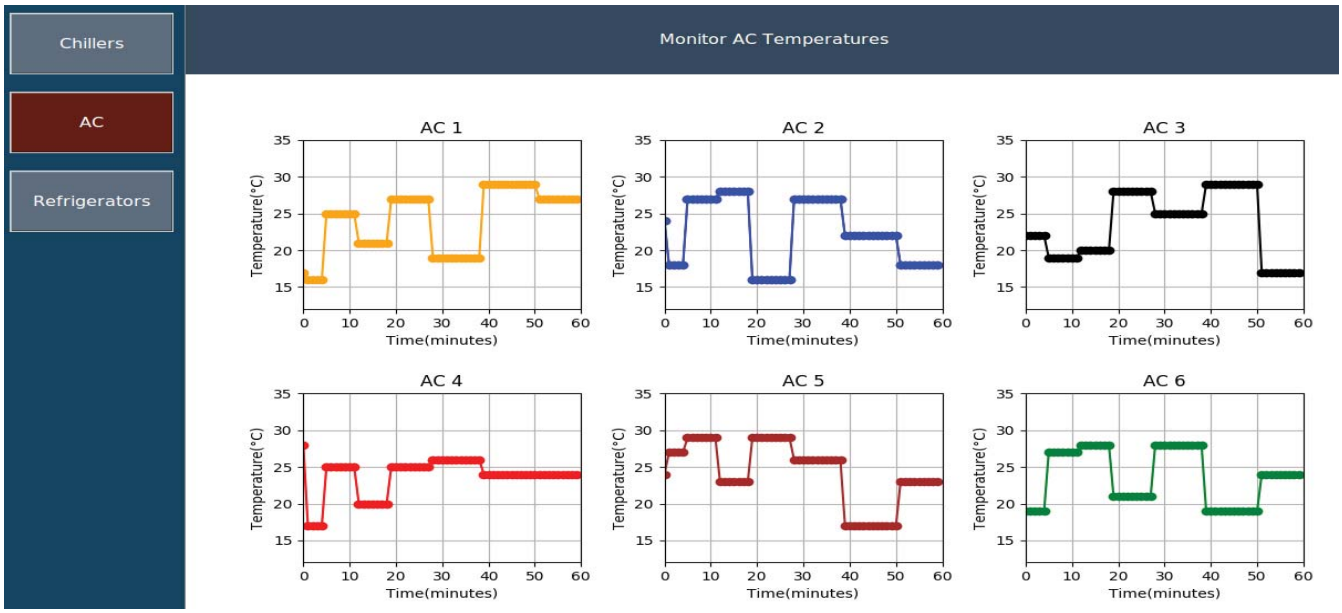
The software has both monitoring and controlling aspects. The most important function of the software is to monitor the system for different hardware components. All types of hardware can be monitored separately as illustrated in Fig. 7. The real-time data published in MQTT broker are retrieved by the software as a client and shown in graphical format in the software preview. The second main function of the software is to send controlling signals to the MQTT broker that is accessible to the respective hardware stations.

E. Database Management

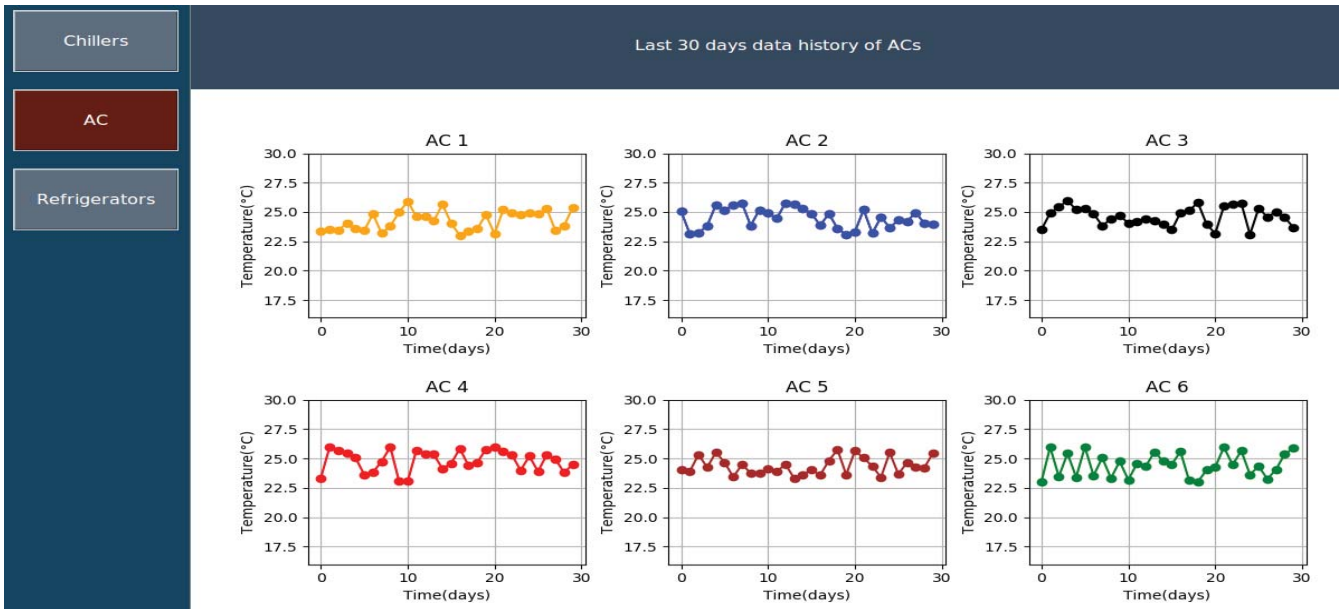
The software saves the real-time data of the hardware components locally for further analysis. These data are used to train the system for improving its decision taking capability and hence automatic control. The historical data can be previewed in the software.

IV. Conclusion

This paper has proposed an offline system for monitoring and controlling of ACs and chillers using MQTT. The whole system is custom built to meet the demands of monitoring and controlling of a real time environment. The system can be employed in any kind of environment. The main advantage of the



(a)



(b)

Fig. 7. Monitoring ACs for the last (a) 60 minutes and (b) 30 days data in the software. Each category of appliances can be monitored separately. Individual appliances can be inspected and monitored from the software.

system is that the system need not to be connected to the data network or Internet for exchanging data with the outside world. A simple intra-network is enough for its operation. As a result, the proposed system is also secured and can't be accessed from illegal software or other networks. Furthermore, the system is intelligent enough to take decisions to control the ambient features and it can be made matured enough by analyzing and training through the historical real-time data saved locally. Nevertheless, the software station is completely isolated from the hardware equipment and does not need to be physically connected to any component. Consequently, the software can be installed in any computer at any place in the arena.

References

[1] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, no. 2011, pp. 1–11, 2011.

[2] M. Dunn, "The next generation of smart fridges." January 2017, [Visited on; 2019-02-27]. [Online]. Available: http://www.news.com.au/technology/gadgets/the-next-generation-of-smart-fridges/news-story/7b75572b8cfbe90432754c8b76abc017

[3] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[4] M. Miller, *The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world*. Pearson Education, 2015.

[5] S. Angal and R. Mali, "Raspberry pi and arduino based automated irrigation system," *International Journal of Science and Research (IJSR)*, vol. 5, no. 7, pp. 1145–1148, 2016.

[6] A. Niruntasukrat, C. Issariyapat, P. Pongpaibool, K. Meesublak, P. Aiumsupucgul, and A. Panya, "Authorization mechanism for mqtt-based internet of things," in *2016 IEEE International Conference on Communications Workshops (ICC)*. IEEE, 2016, pp. 290–295.

[7] N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, and G. Reali, "Comparison of two lightweight protocols for smartphone-based sensing," in *2013 IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*. IEEE, 2013, pp. 1–6.

[8] Y. Upadhyay, A. Borole, and D. Dileepan, "Mqtt based secured home automation system," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*. IEEE, 2016, pp. 1–4.

[9] M. organization, "Mqtt software package," July 2009, [Visited on; 2019-02-27]. [Online]. Available: http://mqtt.org/

[10] S. Tarkoma, *Publish/subscribe systems: design and principles*. John Wiley & Sons, 2012.

[11] P. Paganini, "Bashlite botnets peaked 1 million in- ternet of thing devices." September 2016, [Visited on; 2019-02-27]. [Online]. Available: http://securityaffairs.co/wordpress/50824/iot/bashlite-botnets.html

[12] I. O. for Standardization, *Ergonomics of the Thermal Environment: Analytical Determination and Interpretation of the Thermal Comfort Using Calculation of the PMV and PPD Indices and Local Thermal Comfort Criteria*. ISO, 2005, pp. 1–52.

[13] W. N. Schofield, "Predicting basal metabolic rate, new standards and review of previous work." *Human Nutrition. Clinical Nutrition*, vol. 39, pp. 5–41, 1985.

[14] S. Cheshire and M. Krochmal, "Multicast dns," Tech. Rep., 2013. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6762.txt

[15] K. Shirriff, "Esp8266 ir remote library." https://github.com/markszabo/IRremoteESP8266, April 2017, [Visited on; 2019-02-27].