ISSN 2278-3091
Volume 9, No.1.1, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse5791.12020.pdf
https://doi.org/10.30534/ijatcse/2020/5791.12020

Intelligent Bothouse: Trend of Development of Industry 4.0

Ruhaya Ab. Aziz, Chan Kah Chun, Hanayanti Hafit, Adila Firdaus Arbain
[1]Software Engineering Department, Faculty Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
*E-mail:ruhaya@uthm.edu.my

:

ABSTRACT

The purpose of this paper is to accommodate the current trend of focusing on the development of Industry 4.0. This is by making a computer, a computer-controlled robot or a software thinks intelligently, in the similar manner the intelligent human thinks. Also, the project is designed to correct problem regarding the incremental total number of house breaks ins. This project is conducted through a series of phases within Evolutionary Prototyping software process. In this paper, intelli-gent-BotHouse system is a minor invention to overlap with Industry 4.0 which is an automated industry. The intelligent-BotHouse system is a smart security house system which allows house member to manage, control and monitor a home environment. First and foremost, this system allows house members to access the system through three main interfaces namely, the physical intact, the mobile platform or the web page provided the given inputs are the correct security re-quirements. The house members can then control the house appliances, house security features and safety monitoring sensors without any location constraints. As a result, house members are able to connect to their house even if they are far away. Eventually, the house members are alerted with the hazards, the threats and the information inside of a house. At the end, the probability of burglary crime, lost of valuable property, hazard, accident or any in-house harmful scenario is minimized. Ease of managing house environment with the pre-set wireless connection can be executed using only a mobile Android smartphone or a computer-based device.

Key words : Smart House, Intelligent System.

1. INTRODUCTION

In Malaysia, crime index recorded a 4.6% increase between January and April in the year of 2016 and the number of burglary cases is still increase until today [1]. It was reported that a total of 38,877 crimes involving properties occurred in Malaysia. In the beginning of the year 2016, 6,662 house breaks ins were reported [1]. The rising number of residential burglary has a close relationship with the criminals' ability and technology advancement in assisting them to pick locks and surpass the victims' home security systems [1]. As a result, home security system is designed and implemented in residential area which intends to reduce the rate of suffering property lost and life protection purpose. This type of system provides immediate and quick signal to the surrounding area so that action can be taken by neighborhood against the burglary. Smart house is implemented to provide more convenient living style in a house by enabling controllable electronic devices wirelessly. It is able to interact with house security system to make it more viable and efficient in a house. House safety monitoring system allows house members to specifically identify and manage the internal home environment through the web page created and integrated with the smart house system.

Most of the existing home security systems are focused on door lock system. Door lock system in hotel management organization using Radio-frequency Identification (RFID) approach embedded in an electronic card is among the best instances. Some of these door lock systems came with a set of 3x3 keypad or 4x4 keypad for entering pin number. It prompts the user to enter pin number which is set by the owner to lock or unlock the door. This approach is able to enhance the level of convenience instead of carrying the key all the time. Perhaps, key could be forgotten and left inside the house. This door lock system is greatly implemented in residential area involving large apartments. Advance security house system will embed with surveillance system to record video on the selected vulnerable area. This surveillance system allows the owners to check on their houses frequently through mobile devices. In addition, smart house systems are designed in relation to Internet of Things (IoT). Basic concept of smart house system is to control electronic devices stationary through the use of internet. However, smart house system is still far from expectation because it requires massive number of hardware and software that are costly.

Perhaps, the total number of house breaks ins increased by time due to the ability of criminals to outsmart the available security system. In the era of big data, people could learn and study easily through the access to the networks for the bad and the good purposes. Also, most of the terraced houses in residential areas are not embedded with any security system. For instance, students who are currently further their study in University Tun Hussein Onn Malaysia (UTHM), faced problems related to burglary crime which can lead to the lost of valuable things due to house break ins. Moreover, lack of

house security makes the house breaks problem become worst. In addition, house security systems in those houses are often being left in the state of idle and resulting in less commercial value to the house owner.

Hence, a great potential solution to improve existing solution for security system is proposed in this project. An intelligent smart security house system namely as intelligent-BotHouse (i-BotHouse) system is designed and tested based on the analysis of current trend and situation in Malaysia. The system is a compilation of multiple sub-systems that are interrelated and interacted. A house has multiple point of accessibility and not limited to the front and the back door alone. Motion sensor provided by the system within the house is able to track down the burglary even though different entering strategies by burglary. Once motion sensor or magnetic door sensor is triggered when the system is activated, then the alarm will be activated. Noise generated by the alarm will definitely gather attention and helps from surrounding neighborhood. At the same time, the house members are notified through phone call and messages about the induction of the system. Immediate action can be done with the assistance of police and neighborhood in capturing the criminal. Furthermore, i-BotHouse system is extended with smart house sub-system that most of the sub-systems can be controlled wirelessly using IoT technology. Extra module and functionalities are to be included to increase user's satisfaction such as voice recognition module, temperature and humidity readings, smoke and gas detection, flame detection and analysis of reports.

The rest of the paper is organized as follows. Section II reviews the necessary terms, concepts and general related work in existing system as well as documentation of every important existing documents, requirements elicitation information and comparison between the chosen existing systems. Section III delineates the methodology used along the software development life cycle (SDLC) processes in achieving the goals of the project through 5 major phases. Section IV presents the analysis and design of the system. It comprises the analytical and technical investigation of the requirements sources. These requirements sources are structured and interpreted in the form of visual diagram. Section V concludes this paper

2. RELATED WORK

2.1 Internet of Things

According to Cluster of European research projects on the IoT, 'Things' are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real or physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention [2]. The Internet of Things is defined in three paradigms – internet-oriented (middleware), things-oriented (sensors) and semantic-oriented (knowledge) [3]. It is said that the usefulness of IoT can be utilized in an application domain where the three paradigms intersect due to the interdisciplinary nature of the subject [4]. It is related to the developed system which it involves the security house system, house safety management system in ensuring the safety and healthy environment within a house, smart house system in controlling utilities and appliances. House or personal users are the entities who interact with the system through the network. This built up the IoT environment and relationship between the three paradigms.

2.2 Smart House System

According to Forrester, a smart environment uses information and communication technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient [5]. A smart house is an application of ubiquitous computing in which the home environment is monitored by ambient intelligent to provide context-aware services and facilitate remote home control [6]. In other words, a smart house is a house comprises of multiple environment monitoring devices that can generate data analyzed from the surrounding environment and control wirelessly with the use of technology generally to provide comfort, healthcare and security services to their inhabitants. To simplify, a smart house is a house equipped with many electronic devices that can be controlled by a mobile device or a computer in order to provide convenient to the house users. The result of a smart house system is correlated to the smart environment definition with the intension to promote the ease of controlling and monitoring home environment in a more efficient method.

2.3 Security House System

A security system is purposely for detecting and signalling the presence of abnormal security or hazardous conditions, such as unauthorized entry, glass breakage, fire, smoke, high water level, in individual units, such as a boat, a recreational vehicle, an automobile, which are located or stored in a given area [7]. A security system has a close relationship with sensors and actuators as they are the devices in controlling the transmission of data assembled from the surrounding environment. In the developed system, 2 major devices are used and contributed to the security features. Passive Infrared Sensor (PIR) or motion detector is an electronic sensor device used to measure Infrared (IR) light that is reflected from an object. It is believed that most of the living things emit heat energy to the surrounding in the form of radiation. However, human naked eyes could not able to detect or see the radiation deviated from the living objects. Instead, this PIR could able to detect the infrared radiation released by or reflected from the objects. Once the PIR detects a digital value fluctuation, for instance, from 0 to 1, it indicates the existence of a living object that emitted heat energy. Thus, it is convenient and

suitable to be installed in the interior of a house to detect any possible unauthorized entry into the house.

Next, reed switch or Heckon or magnetic door sensor is an electronic device operated in the form of magnetic field. It comes with a pair and only one side is connected with wire. Electrical energy supplies to this reed switch will be converted to the magnetic force and formed magnetic field between the reed switch. Magnetic field distorted by the movement of door such as opening the door will result in the digital value changes. This indication is used to identify house breaks in and trigger the alarm through the fluctuation of digital value pin.

2.4 House Safety Monitoring System

House safety monitoring system allows users to check frequently on the safety level in a house. This system often composes of numerous sensors integrated and installed in a house. These sensors are created to read or measure the surrounding environment changes. Users will be able to take immediate action through the notification received from the monitoring system whenever environment changes hit the threshold level of danger or hazards occurred. These hazards cannot always be avoided, but damage from them can be limited if prompt notification is given when they occur [8]. Few of those modules are selected based on its capabilities and appropriate in implementing the developed system. One of them is gas sensor (MQ-2) used specifically to detect gas leakage in home. It can detect hydrogen gas, liquefied petroleum gas (LPG), methane gas, carbon monoxide, alcohol, smoke or propane gas. By default, it is very sensitive to the type of gases as mentioned and provided fast responses. Readings are changed very quickly and can be measured in a shorter period of time.

Moreover, flame sensor is an electronic device used to detect fire source within a specific range of wavelength. According to the user manual of flame sensor, it can measure and detect flame source wavelength in the range of 760nm to 1100nm. Flame sensor is installed and used in monitoring the house safety environment despite the available of gas sensor. This is because a flame sensor is usually response faster and accurately than the gas sensor as it is specifically made to detect flame changes.

3. RESEARCH METHODOLOGY

This section discusses about the approach and methods used in this study.

3.1 Software Process Model

Prototyping model is one of the rapid application developments within the software development life cycle (SDLC). Software or system prototyping has many variants. In this project, Evolutionary Prototyping is applied rather than choosing the Throwaway Prototyping. This is because design prototyping is not intended to be the real or actual working system in Throwaway Prototyping. It includes the development of prototype. However, the developed prototype is used to validate with the requirements of the user regarding the features, conditions and capabilities implied within the prototype. It contains brief details in user involvements. Perhaps, Evolutionary Prototyping is another prototyping approach used to build a large scale prototype in a structured pattern. It is then continuously honed from time to time. This genre of software prototyping or system prototyping promotes constant enhancement, improvement, refinement, features increment and changes based on relevant customer requirements and change requests. Also, it provides risk management control through identifying and eliminating faults in the primary version of prototype. Evolutionary Prototyping is absolute reducing time and cost. This prototyping can constantly improve the system requirement specification (SRS) through user involvement. Changes made at the end of the project development are expected to be exclusively expensive as compared to identification of changes through constant involvement of user in the midst of the project development. Another reason will be user involvement. The incremental rate of user involvement will definitely influence proportionally the satisfaction level of user about the requirements discussed. Interaction of user to the prototype provides instant feedback and the developer will be able to design and develop a prototype which is closer to a complete deliverable. Also, verification and validation can be executed by user which will prevent misunderstandings and miscommunications due to misinterpretation between the developer and the user. Since users know what the users want more than anyone else, increased number of interactions will yield better value of tangible and intangible quality for the final product. As a result, the deliverable is more likely to be accepted and satisfied the user. System prototyping comprises of 4 main phases namely planning phase, analysis phase, design phase and implementation phase. Figure 1 depicts Evolutionary Prototyping model with its phases or stages.

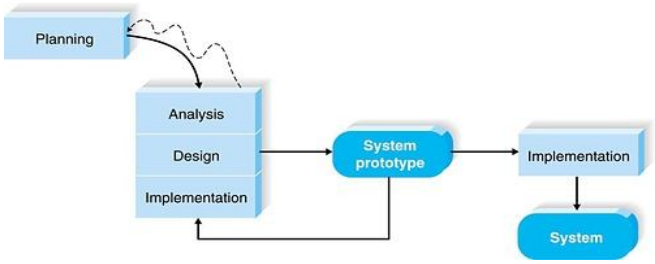

Figure 1: Evolutionary Prototyping model with its phases or stages

There are total of eleven phases while processing the evolutionary prototyping model. According to Table 2, each phase was decomposed into more concrete and specific activities which were performed along the software development process. Outputs are the results from completion of the work breakdown components. In the end, all the tasks had been executed and documented based on the initial project

development planning and project scope development with accomplishment of triple constraints, scope, time and cost goals.

4. ANALYSIS & DESIGN

Requirements that are elicited as mentioned in system development workflow are recorded and documented in compliance with documentation rules or guidelines. These requirements are represented in various forms of diagrams and tables which include the Data Flow Diagram Context Diagram (DFD CD), Data Flow Diagram Level 0, Requirement Traceability Matrix (RTM) and Entity Relationship Diagram (ERD).

4.1 DFD Context Diagram

This DFD Context Diagram comprises of 3 main elements. There are entity, data flows and the main process. Data store is not reviewed in Context Diagram but in higher level of DFD diagrams. All these elements are shown in Figure 2.

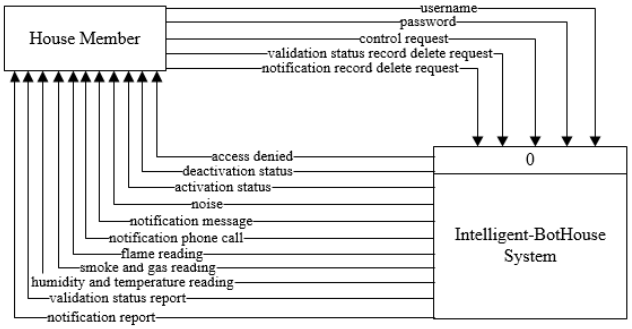

Figure 2: Level of DFD diagrams

4.2 DFD level 0

In this sub-section, the main process is further decomposed into 8 more concrete processes offered by the system. Observe that the total number of data flow in and data flow out of the entity house member in DFD Context Diagram is equivalent to the total number of data flow in and data flow out of the entity house member in DFD Level 0. All the data flows are then classified and divided into different specific processes which the processes required the particular data flow. In addition, data stores are shown in the DFD Level 0 which represents the data or information are being stored and used in different processes when necessary. These data store are named as User, Access_Validation, Notification_Report.

4.3 Requirements Traceability Matrix

Based on the main scenario and alternative scenario in the Process Specifications, requirements are identified, analyzed, elicited and documented in Table 1.

Table 1: Requirement Traceability Matrix

Requirement	Description
SRS_REQ_100	**Access the System**
SRS_REQ_101	The system shall allow house members to input pin number physically on the membrane keypad.
SRS_REQ_102	The system shall allow house members to set up pairing password for Bluetooth module.
SRS_REQ_103	The system shall allow house members to enter username and password through log in interface on a web page.
SRS_REQ_104	The system shall allow house members to enter username and password through log in interface of a mobile application.
SRS_REQ_105	The system shall allow house members to reset pin number input from a membrane keypad.
SRS_REQ_106	The system shall allow house members to submit pin number or username and password.
SRS_REQ_107	The system shall validate the pin number or username and password.
SRS_REQ_108	The system shall display a new menu option if pin number input matched with the system.
SRS_REQ_109	The system shall display a new interface if correct and valid username and password input after submitted
SRS_REQ_110	The system shall display error message if invalid pin number detected or incorrect username and password submitted.
SRS_REQ_111	The system shall record the access status into the database
SRS_REQ_112	The system shall record the access date and time into the database.
SRS_REQ_200	**Manage Devices or Sensors**
SRS_REQ_201	The system shall allow the house members to activate full house security system via toggle button in a mobile application.
SRS_REQ_202	The system shall allow the house members to deactivate full house security system via toggle button in a mobile application.
SRS_REQ_203	The system shall allow the house members to activate full house security system via button in a web application.
SRS_REQ_204	The system shall allow the house members to deactivate full house

	security system via button in a web application.
SRS_REQ_205	The system shall allow the house member to activate full house security system via the physical membrane keypad menu selection.
SRS_REQ_206	The system shall allow the house member to deactivate full house security system via the physical membrane keypad menu selection.
SRS_REQ_207	The system shall display activation message on the LCD for full house security system.
SRS_REQ_208	The system shall display deactivation message on the LCD for full house security system.
SRS_REQ_209	The system shall allow the house members to activate door security system via toggle button in a mobile application.
SRS_REQ_210	The system shall allow the house members to deactivate door security system via toggle button in a mobile application.
SRS_REQ_211	The system shall allow the house members to activate door security system via button in a web application.
SRS_REQ_212	The system shall allow the house members to deactivate door security system via button in a web application.
SRS_REQ_213	The system shall allow the house member to activate door security system via the physical membrane keypad menu selection.
SRS_REQ_214	The system shall allow the house member to deactivate door security system via the physical membrane keypad menu selection.
SRS_REQ_215	The system shall display activation message on the LCD for door security system.
SRS_REQ_216	The system shall display deactivation message on the LCD for door security system.
SRS_REQ_217	The system shall allow the house members to activate smoke and gas detector via toggle button in a mobile application.
SRS_REQ_218	The system shall allow the house members to deactivate smoke and gas detector via toggle button in a mobile application.
SRS_REQ_219	The system shall allow the house members to activate smoke and gas detector via button in a web application.
SRS_REQ_220	The system shall allow the house members to deactivate smoke and gas detector via button in a web application.
SRS_REQ_221	The system shall allow the house members to activate flame detector via toggle button in a mobile application.
SRS_REQ_222	The system shall allow the house members to deactivate flame detector via toggle button in a mobile application.
SRS_REQ_223	The system shall allow the house members to activate flame detector via button in a web application.
SRS_REQ_224	The system shall allow the house members to deactivate flame detector via button in a web application.
SRS_REQ_225	The system shall allow the house members to activate humidity and temperature sensor via toggle button in a mobile application.
SRS_REQ_226	The system shall allow the house members to deactivate humidity and temperature sensor via toggle button in a mobile application.
SRS_REQ_227	The system shall allow the house members to activate humidity and temperature sensor via button in a web application.
SRS_REQ_228	The system shall allow the house members to deactivate humidity and temperature sensor via button in a web application.
SRS_REQ_229	The system shall allow the house members to switch on light via toggle button in a mobile application.
SRS_REQ_230	The system shall allow the house members to switch off light toggle button in a mobile application.
SRS_REQ_231	The system shall allow the house members to switch on light via button in a web application.
SRS_REQ_232	The system shall allow the house members to switch off light via button in a web application.
SRS_REQ_300	**View Status Review**
SRS_REQ_301	The system shall response on full house security system activation status in the status review and in the home page of the web application.
SRS_REQ_302	The system shall response on full house security system deactivation

	status in the status review and in the home page of the web application.
SRS_REQ_303	The system shall response on door security system activation status in the status review and in the home page of the web application.
SRS_REQ_304	The system shall response on door security system deactivation status in the status review and in the home page of the web application.
SRS_REQ_305	The system shall response on smoke and gas detector activation status in the status review and in the home page of the web application.
SRS_REQ_306	The system shall response on smoke and gas detector deactivation status in the status review and in the home page of the web application.
SRS_REQ_307	The system shall response on flame detector activation status in the status review and in the home page of the web application.
SRS_REQ_308	The system shall response on flame detector deactivation status in the status review and in the home page of the web application.
SRS_REQ_309	The system shall response on humidity and temperature sensor activation status in the status review and in the home page of the web application.
SRS_REQ_310	The system shall response on humidity and temperature deactivation status in the status review and in the home page of the web application.
SRS_REQ_311	The system shall response on the light activation status in the status review and in the home page of the web application.
SRS_REQ_312	The system shall response on the light deactivation status in the status review and in the home page of the web application.
SRS_REQ_400	**Analyze Devices or Sensors Readings**
SRS_REQ_401	The system shall read the heat value in the surrounding environment within the house while the flame detector is activated.
SRS_REQ_402	The system shall read the smoke and gas concentration in the surrounding environment within the house while the smoke and gas detector is activated.
SRS_REQ_403	The system shall read the humidity and temperature in the air within the house while the humidity and temperature sensor is activated.
SRS_REQ_404	The system shall display the flame reading in the home page of the web application.
SRS_REQ_405	The system shall display the smoke and the gas reading in the home page of the web application.
SRS_REQ_406	The system shall display the humidity and the temperature reading in the home page of the web application.
SRS_REQ_407	The system shall detect magnetic door analog reading changes while the magnetic door sensor is activated
SRS_REQ_408	The system shall detect motion analog reading changes while the motion detector is activated
SRS_REQ_409	The system shall detect dangerous level of flame reading or high value of flame reading while the flame detector is activated
SRS_REQ_410	The system shall detect dangerous level of smoke and gas reading or high value of smoke and gas reading while the smoke and gas detector is activated
SRS_REQ_500	**Generate Buzzer Noise**
SRS_REQ_501	The system shall generate buzzer noise if object motion is detected in house while the motion detector is activated.
SRS_REQ_502	The system shall generate buzzer noise if door movement is detected in house while the magnetic door sensor is activated.
SRS_REQ_503	The system shall generate buzzer noise if leaking gas is detected in house while smoke and gas detector is activated.
SRS_REQ_504	The system shall generate buzzer noise if high smoke concentration is detected in house while the smoke and gas detector is activated.
SRS_REQ_505	The system shall generate buzzer noise if flame outbreak in house is detected while the flame detector is activated.
SRS_REQ_600	**Send Notification**
SRS_REQ_601	The system shall send notification message and make empty phone call to inform house member if object motion is detected in house while the motion detector is activated.

SRS_REQ_602	The system shall send notification message and make empty phone call to inform house member if door movement is detected in house while the magnetic door sensor is activated.
SRS_REQ_603	The system shall send notification message and make empty phone call to inform house member if leaking gas is detected in house while the smoke and gas detector is activated.
SRS_REQ_604	The system shall send notification message and make empty phone call to inform house member if high smoke concentration is detected in house while the smoke and gas detector is activated.
SRS_REQ_605	The system shall send notification message and make empty phone call to inform house member if flame outbreak in house is detected while the flame detector is activated.
SRS_REQ_700	**Manage Notification Report**
SRS_REQ_701	The system shall display notification description in the notification report table.
SRS_REQ_702	The system shall display the notification date and time in the notification report table.
SRS_REQ_703	The system shall allow house members to delete undesired record of notification report table.
SRS_REQ_800	**Manage Validation Status Report**
SRS_REQ_801	The system shall display the access status in the validation status report table.
SRS_REQ_802	The system shall display the access date and time in the validation status report table.
SRS_REQ_803	The system shall allow house member to delete undesired record of validation status report table.

4.4 Entity Relationships Diagram

By referring to the data stores created in Data Flow Diagram Level 0, the Entity Relationship Diagram is modelled. Total of four entities are created. The entities are User, Access_Validation, Notification_Report and House Member. Figure 3 portrays the Entity Relationship Diagram for intelligent-BotHouse system.

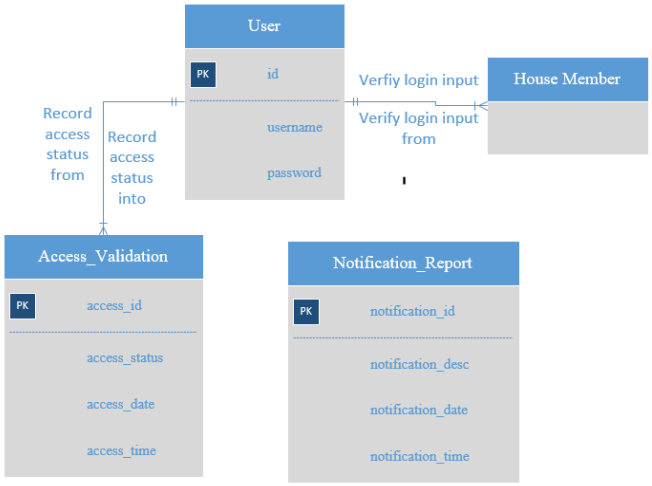

Figure 3: Entity Relationship Diagram for intelligent-BotHouse system

4.5 System Interfaces

In this section, interface designs of the system are discussed and displayed. These interface designs are designed based on the processes from the previous section.

1) *Process Access The System*

Figure 4 and Figure 5 display the interface designs for process *Access the System* in the Android smartphone application and web-based application.

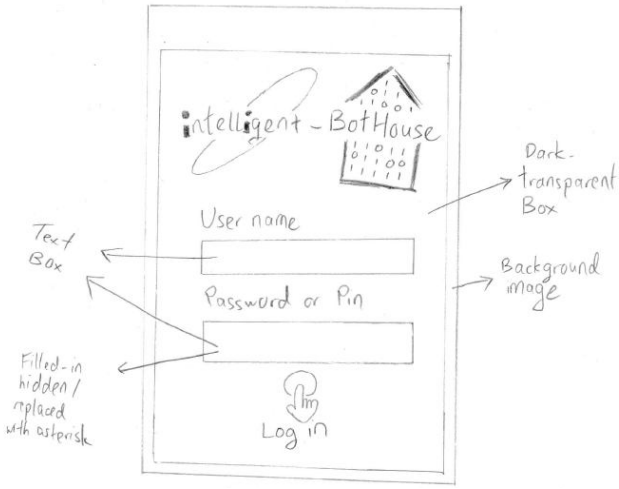

Figure 4: Login interface for Android smartphone application

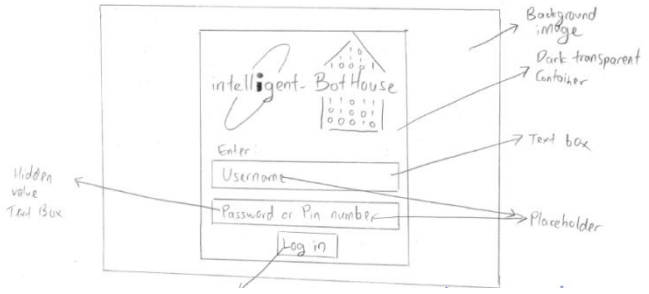

Figure 5: Login interface for web-based application

2) Process Manage Devices or Sensors

Figure 6 shows the interface design for all the control processes in the mobile application whereas Figure 7, Figure 8 and Figure 9 depict the interface designs for process *Manage Devices or Sensors* in the web-based application.

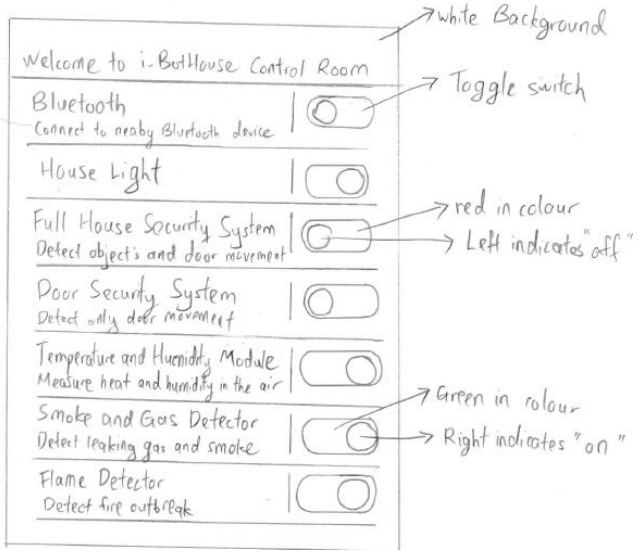

Figure 6: Security control interface for Android smartphone application

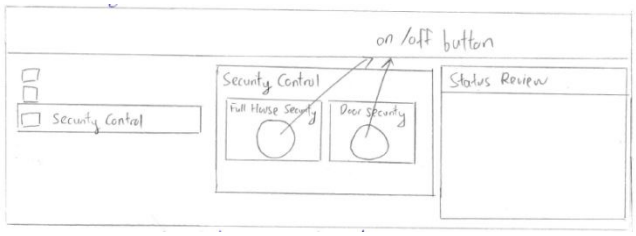

Figure 7: Security control interface for web-based application

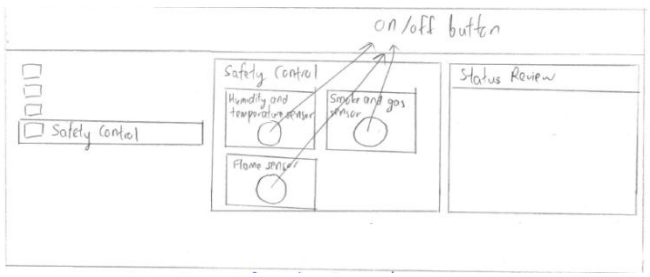

Figure 8: Safety control interface for web-based application

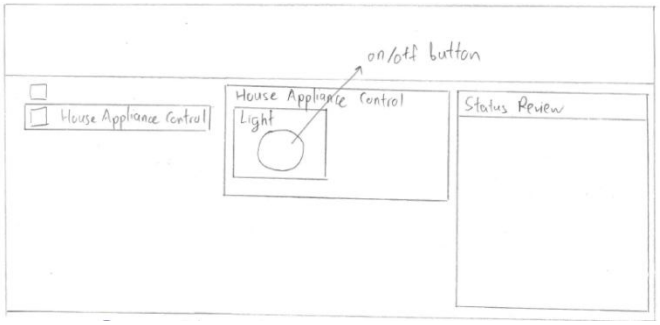

Figure 9: House appliance control interface for web-based application

3) Process View Status Review

Figure 10 portrays the interface design for process *View Status Review* in the web-based application.

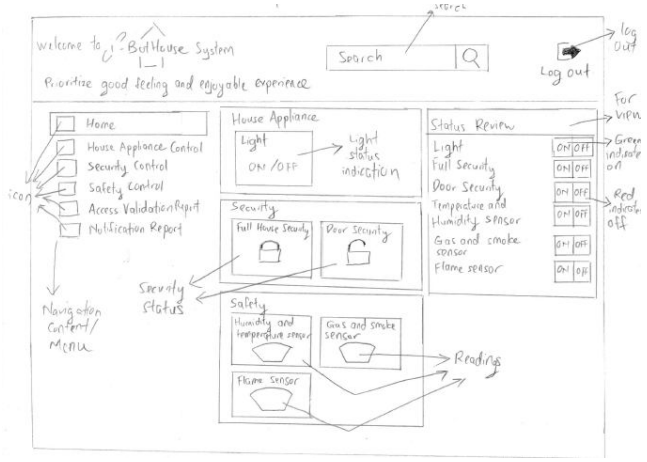

Figure 10: Status Review on the right side of the interface design for web-based application

4) Process Analyze Devices or Sensors Readings

Figure 11 shows the interface design for process *Analyze Devices or Sensors Readings* or the home page in the web-based application.

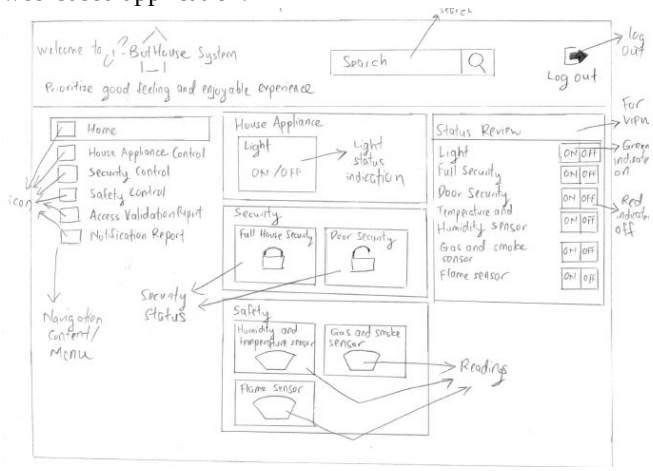

Figure 11: Home page for the web-based application

5) Process Manage Notification Report

Figure 12 shows the interface design for process *Manage Notification Report* in the web-based application.

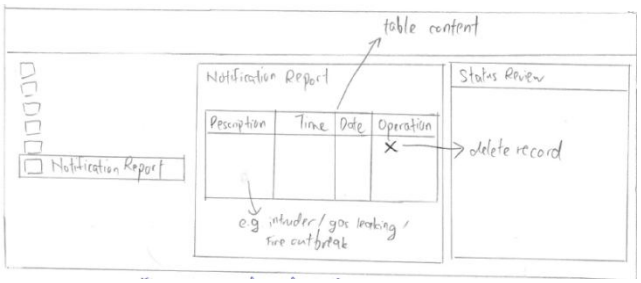

Figure 12: Notification report or analysis report screen for web-based application

6) Process Manage Notification Report

Figure 13 shows the interface design for process *Manage Validation Status Report* in the web-based application.

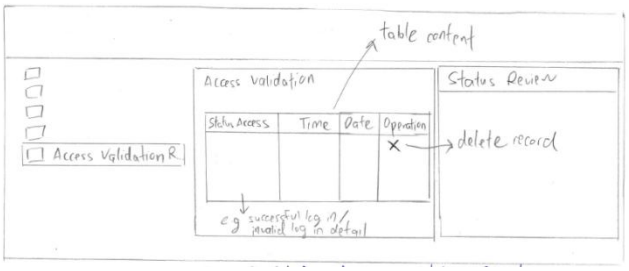

Figure 13: Access validation screen for the web-based application

5. IMPLEMENTATION

The prototype design of the system is implemented based on the documents or formal specification created during the Analysis and Design phase.

A. *Access the System Interface*

In web-based application design, the main interface design of the intelligent-BotHouse to redirect to the sign in page is shown in Figure 14. By clicking on the sign in button, the web page will be redirected to the sign in page in order to gain access to the smart home control system. Figure 15 shows the login interface.

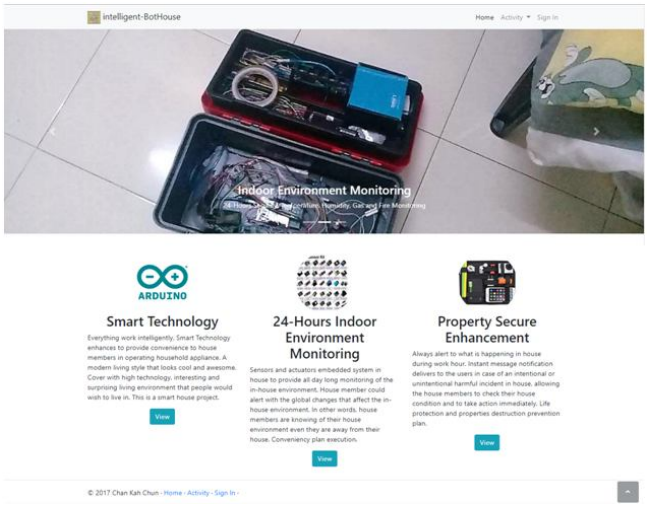

Figure 14: Main interface for intelligent-BotHouse

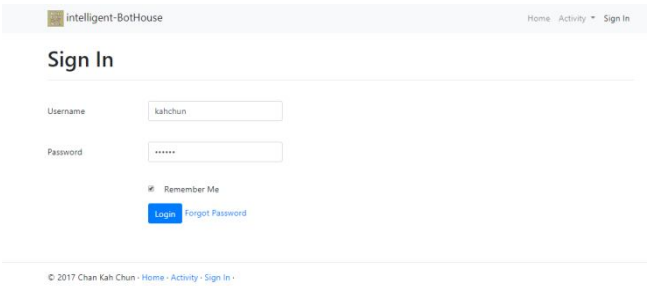

Figure 15: Sign in interface

B. *Manage Devices or Sensors Interface*

In this sub-section, all the system control interfaces are displayed. The first interface to be portrayed in Figure 16 is the house appliance control interface. Figure 17 reviews the security control interface. Figure 18 shows the fire detection detection control interface. Figure 19 displays the humidity and temperature monitor control interface and Figure 20 indicates the gas concentration monitor control interface.

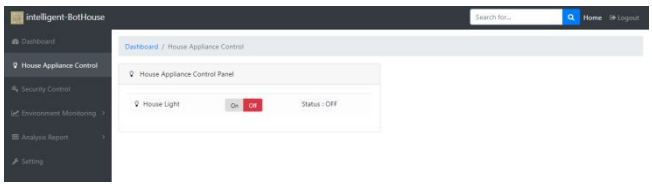

Figure 16: House appliance control interface

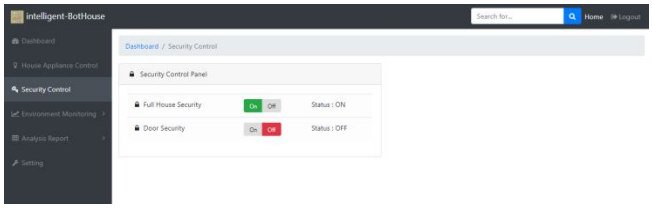

Figure 17: Security control interface

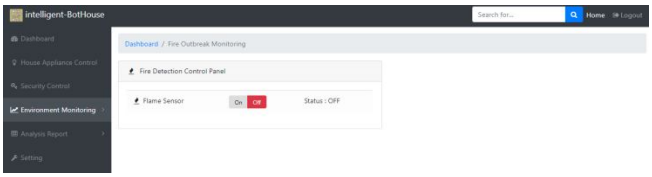

Figure 18: Fire detection control interface

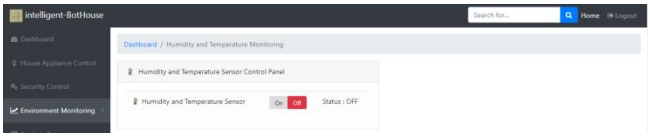

Figure 19: Humidity and temperature monitor control interface

Figure 20: Gas concentration monitor control interface

C. *View Status Review Interface*

The dashboard web interface displays the main control panel or the status review interface. Figure 21 indicates its interface.

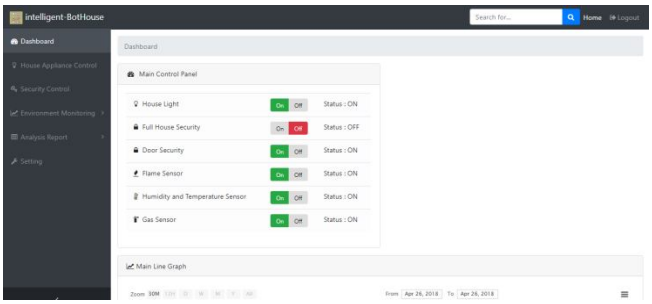

Figure 21: Main control panel or status review interface

D. *Analyze Devices or Sensors Readings Interface*

In this particular module, the data that the sensors gather are sent to the thingspeak cloud server and the data is represented in the graph within the tab of public or private view. These graphs are used in the web interface to read the information and reorganized the information into more comprehensive line graph and combination of multiple graphs. This is shown in Figure 22 and 23.

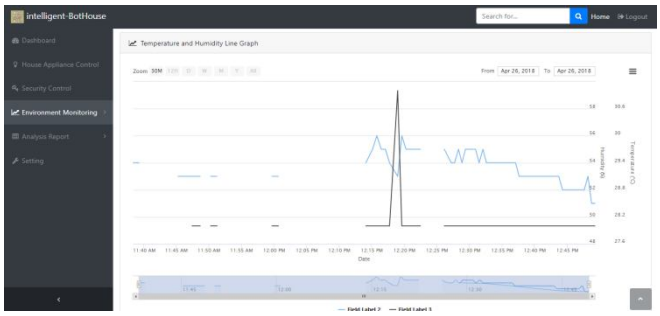

Figure 22: Humidity and temperature line graph interface

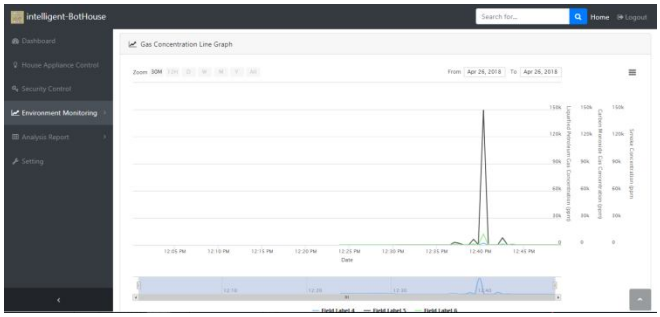

Figure 23: Gas concentration line graph interface

E. *Send Notification Interface*

After alarm is triggered due to safety and security measures, the message-based notification will be delivered to the users. Figure 24 depicts the illustration of the message received by user.

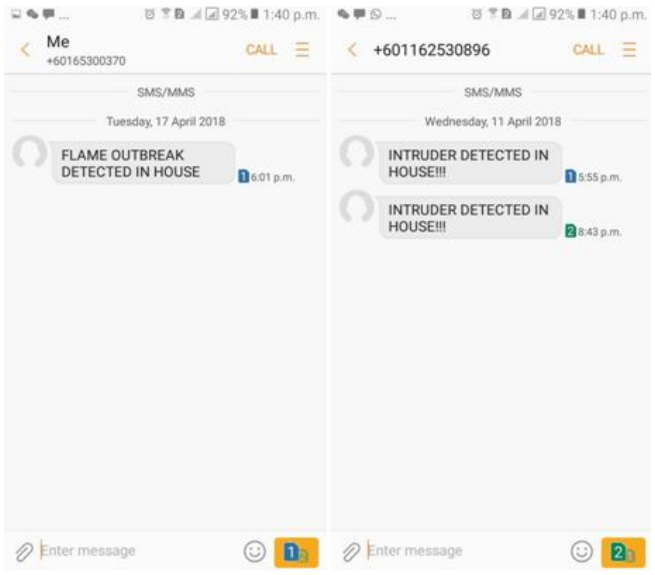

Figure 24: Alert message notification example

F. *Manage Notification Report Interface*

Notification sent from the GSM to the user creates a record and save into the database. These information are then displayed in the web page through read mechanism from

database table. User can conduct delete operation on selected record in the table as shown in Figure 25.

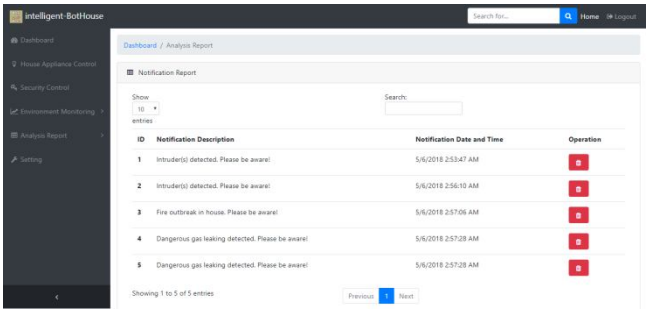

Figure 25: Notification report interface

G. *Manage Validation Status Report Interface*

Each login procedure will records its status, date and time into the database. These information will be presented in the access validation report table for user to check and ensure no hacker is trying to attack the web interface. Also, User can conduct delete operation on selected record in the table as shown in Figure 26.

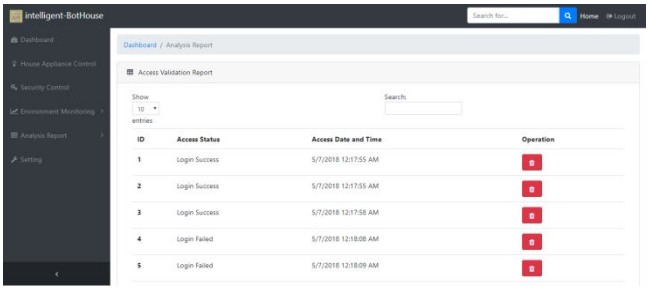

Figure 26: Access validation report interface

6. TESTING

A total of 53 test cases were designed to test the whole system. The system passed 51 test cases which is equivalent to 96.23% of the total test cases. Table 2 portrays the overall result of the test cases.

Table 2: Overall Test Result

ID	Total Test Cases	Total Number of Passes
STD_TEST_100	8	7
STD_TEST_200	15	15
STD_TEST_300	6	6
STD_TEST_400	10	9
STD_TEST_500	5	5
STD_TEST_60	5	5
0		
STD_TEST_700	2	2
STD_TEST_800	2	2
	53	51

7. CONCLUSION

This project has been a great driven force for developing something great in the predetermined time frame. In the current development progress, focus is more on the functions rather than the interface design. This is because smart house system without its functions is no longer a smart house system. With the available of Internet, smart house is enhancing towards to Industry 4.0 trend which involves intelligent automated machine or robot for industry operation.

ACKNOWLEDGEMENT

The authors fully acknowledged Ministry of Education (MOE) and Universiti Tun Hussein Onn Malaysia for the approved fund which makes this important research viable and effective.

REFERENCES

[1] Shahrudin, H. S. “Malaysia’s crime index sees 4.6 per cent increase.” Retrieved from http://www.nst.com.my/news/2016/05/144196/malaysias-crime-index-sees-46-cent-increase (2016). [Accessed : 2-Apr-2017]

[2] Sundmaeker, H., et al. "Vision and challenges for realising the Internet of Things." *Cluster of European Research Projects on the Internet of Things, European Commision* 3.3 (2010): 34-36.

[3] Atzori, L., Iera, A., and Morabito, G. "The internet of things: A survey." *Computer networks* 54.15 (2010): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[4] Gubbi, J., et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7 (2013): 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[5] Bélissent, J. "Getting clever about smart cities: new opportunities require new business models." *Cambridge, Massachusetts, USA* (2010).

[6] Alam, M.R., Ibne Reaz, M. and Mohd Ali, M.A. "A review of smart homes—Past, present, and future." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 42.6 (2012): 1190-1203. https://doi.org/10.1109/TSMCC.2012.2189204

[7] Glidewell, W. E., Furr III, E. F., and Witham, M.J. "Security system." U.S. Patent No. 5,319,698. 7 Jun. 1994.

[8] Albert, D. E. “Security system.” U.S. Patent No. 7,173,525. 2007.