Security Testing of IoT Smart Applications

Shymaa Sobhy
Department of Computer Science
Faculty of Computers and Information
Menofia University
{shaymaa.abdelaal@ci.menofia.edu.eg}

Eman M.Mohamed
Department of Computer Science
Faculty of Computers and Information
Menofia University
{eman.mohamed@ci.menofia.edu.eg }

Arabi Keshk
Department of Computer Science
Faculty of Computers and Information
Menofia University
{arabi.keshk@ci.menofia.edu.eg}

***Abstract*--Internet of Things (IoT) offers a big variety of smart applications. Smart homes (SH) are a well-known utility of IoT that enhances quality of life. Security is the main challenge when discussing IoT due to the fact that it's far reachable across the world. Thus protecting SH against unauthorized customers may be very vital. Having access to sensor datasets is vital for SH research. Cost, time, low quality, and amount of present sensor datasets make it difficult for researchers to acquire data sets. SH simulation is a method to solve those problems. This paper proposes to enhance an existing SH simulation tool to be remotely managed inside a secure server. The data sets were created the usage of a hybrid, open-source SH simulator OpenSHS, (Open Smart Home Simulator), for generate data sets. The actions of persons in their life were collected by OpenSHS. The design in OpenSHS can only be managed via the Blender program. For remotely managed through objects in Blender, a web server was developed that automatic return some data on all objects in a designed home and manages far away their properties in a good manner. To upload protection for the server an internet web page turned into designed with password safety to save you unauthorized customers from having access to the server. At the end, the system protection was validated by different four passwords related on their success rate; the confusion matrix was used also for the high secure used password. The results reveal that the proposed method is actually do well prior to the SH research.**

***Keywords*--internet of things; smart applications; smart homes; simulation.**

I. INTRODUCTION

The IoT is a network of devices connected to a common networks to communicate, sending data, or control devices [1]. Devices are such things as sensors and actuators, which might be equipped with telecommunication interfaces, processing units, and low memory. It offers you approach to combine objects on the Internet through developing human-to-tool interactions among devices. It provides you ways to integrate objects on the Internet by creating human-to-device interactions between devices. In addition to having an Internet connection, it additionally has cloud control and data control, protection control, and all other fields associated with the Internet era. A main application of IoT is the SH, surroundings that adapts to its user's requirements [2].

SH studies has in particular centered on the usage of sensors to enhance the strength performance of buildings. SH create smart environments that may assist the customers to carry out their responsibilities for you to enhance their life, to guard them through developing secure environment, or to aid health treatments [3]. When design SH many of sensors turned into related to accumulate data from customers to deal with them. A vital thing to bear in mind is the information location because of connectivity with the energy consumption and the user's activities [4].

With the improvement of the IoT, the evaluation of SH data has attracted greater attention. Services, like anomaly detection, activity classification and recognition, require data sets for results testing and validation [5]. These require actual datasets which are consultant of the eventualities captured from a SH. However, the efforts of constructing an actual SH and every now and then it isn't always possible for real product [6]. addition, researchers nonetheless face many demanding situations earlier than constructing SH, which includes locating a appropriate placement of the sensors, loss of flexibility, locating suitable participants, and private ness and moral issues [7].

The real SH datasets have many troubles, Such as, the want to add more sensors to control the type of the generated scenarios. Some of these data set record sensor readings in actual-time [8]. The data set simulation tool eliminates the problems of creating real data sets. In a real SH, if design need to be changed, it is high price and choice. On the other hand, through simulating a SH, this is straightforward to achieve, and researchers can go back and redesign the SH [9]. SH are an answer for supplying aid to population in finishing every day sports and improving their quality of life. When manage, control is delivered to SH home equipment this reduces human interaction, will increase protection and decreases electricity consumption [10]. With the increase usage of smart devices in the SH, generates great amount of data streams that need to be analyzed. Access to sensor datasets is critical for SH studies. Real SH has problems could make it tough for developer to create data sets, this difficulties are cost, time, inflexibility of real SH, also quantity and quality of real sensor datasets is limited. SH simulation is a method to reduce those limitations and problems [11].

In SH you could manage electronics and home appliances, telecommunications, protection, lighting. SH system offers information on home equipment remotely. The SH customers can get entry to it from far places through smartphone or computer, permitting us to control the heat, for example, on their way home from work. SH systems have to meet the desires of comfort living, existence safety, and protection [13]. Protection of SH layout primarily based totally on IoT applications is a factor that represents an essential count of SH studies. SH devices must be secured and verified against vulnerability for the prevention of security breaches while facing future threats. Security technology that guards IoT data must be at once adopted. Controlling and protecting personal

data are essential elements inside the SH layout. SH protection manage system has become vital in every day like Human face recognition technology and remotely monitoring technology, to confirm visitor identity and to control door accessibility [14].

In this paper, an existing SH simulation for dataset collection was improved to be remotely managed through an internet HTTP server. The data sets are generated the usage of OpenSHS, to create dataset [10]. OpenSHS collect information of customers in digital surroundings [11]. The design in OpenSHS can only be managed through the Blender program [12]. For remotely controlling objects in Blender, an HTTP server was developed to automatically retrieve information for all objects in a scene and changes their properties remotely. Security version turned into delivered that don't permit unauthorized men and women to get entry to the server [15]. Finally protection turned into demonstrated with extraordinary 4 passwords primarily based totally on their success rate and confusion matrix was calculated for the most secure password [16].

The remainder of this paper is ordered as follows. Related work is analyzed in Section 2. The proposed method introduced in Section 3. Section 4 experimental results. Section 5 presents the conclusion.

II. RELATED WORK

This section describes the work related to our method. Also an existing simulation tool was explained in detail that used as a base for our approach.

IoT security testing has been studied intensively in the last years [13] with a particular effort on SH security testing. This study concentrate on the concept of SH as a place of security and control to test how users living in SH and use the home technology to create and maintain a secure space where they can feel in control of their life. The findings suggest that how the relation between householders, smart home technology and external factors is imagined and experienced might be an important factor for whether people feel in control and secure in their homes.

In [14] they describe about the implementation and deployment of wireless control system and accessibility in to the SH for authenticated people only. A wireless network ZigBee based and image processing, makes the security system alive as per the request. Face detection and recognition algorithms, as well as a wireless interface are used to detect and identify visitors and send an email and/or an alert message about the current SH status automatically to the home owner's mobile phone or any communication devices. Users can monitor visitors and control the door lock on active Web pages.

In [16] Smart home control system (SHCS) can be integrated into an existing home appliances to reduce the need for human, increase security and energy efficiency. SH system uses four types of sensors for automatic control and intrusion detection. Performance of system evaluated. Results showed the effectiveness of SH system in the prototype and real life experiments.

The technology efforts concentrate to generate for SH more datasets for subsequent analysis. The simulation tools for SH into two broad categories using two main approaches: model-based and interactive approaches. A third approach combines model-based and interactive simulation; this approach is known as a hybrid. In the following, existing tools for each approach was described [11]. Model-based approaches for the simulation data for the purposes of generating synthetic devices data include specific activity models that determine the arrangement of the events, the likelihood of an event taking place, and the time that the performance of specific activities takes.

Bouchard et al. [17] propose an approach used within the SIMACT simulator. The tool provided a form-based interface for the specification of scripts that detail the series of steps involved in the performance of activities within a SH. Users specify the events order, time, objects and define actions such as the movement of objects. The script can be played in real-time. The object data is stored within a database to create an open-source database example.

Helal et al. [18] introduce the PerSim simulator. PerSim is designed to facilitate data synthesis for activity detection research in testing. The program defines user's actions, sensor activations order, sensor status, and activity duration. They developed library of sensor data that show data activity performance, or for the entire room, such as temperature sensors.

An interactive approach differs from a model-based approach in that it depends on possessing an avatar that a researcher is able to control a human or simulated participant. The Intelligent Environment Simulation (IE Sim) is a tool to capture the normal as well as abnormal ADLs of the occupants [9]. IE Sim grants the investigators to develop SH designing. The investigators are also allowed to add various kinds of sensors, like temperature, pressure sensors. Afterward, with the aid of an avatar, the simulation could be carried out in such a way that it captures ADLs.

Ariani et al. [18] created a tool for SH that made use of ambient devices for capturing the occupant's interactions. The simulation allow researcher to design or creates a flooring scheme similar to the intelligent home through patterning the shapes on a 2D frame; afterward, ambient devices to the virtual home are able to add by the researcher.

The hybrid approach aims to combine the best among approaches. Home I/O [19] is reality program for simulating a SH. Its main target domains are science, mathematics, and engineering. It was designed as a learning tool for new generations of students and teachers. Covering the curriculum targets in Science, Technology, Engineering and Math (STEM), HOME I/O has all tools needed to monitor a real-time SH simulation. OpenSHS is a free tool for dataset creation, [20], which is downloadable from http://www.openshs.org under the GPLv2 license [21]. It was improved to remotely control objects via a secure HTTP server that don't allow unauthorized users to access the server.

III. The Proposed Approach

This phase introduces firstly background about OpenSHS secondly OpenSHS Implementation thirdly the proposed method and system description [9].

A. Background

In this section, two elements were used, the researcher and the participant. Most of the work done by OpenSHS is done by researchers. Participants are anyone who voluntarily simulates their activities. Three main phases: the design phase, the simulation phase, and the aggregation phase.

(1) **Design Phase***:* Researchers create a virtual environment, import smart devices, assign actions to tags, and develop context.
   1) *Design Floor Plan:* The researcher designs the 3D floor plan by using a Blender which allows controlling of dimensions, number of rooms.
   2) *Importing Smart Devices*: a library, offered by OpenSHS full of devices is programmed with Python: Pressure, Door sensors, Lock devices, Appliance switches, and Light controllers.
   3) *Assigning Activity to Labels:* OpenSHS allows researchers to define an unlimited number of action tags. The researcher decides how many labels are needed according to experiment's requirements such as 'sleep', 'eat', 'personal', and 'work' and 'other'.
   4) *Designing Contexts:* After developing the SH model, the researcher creates a context for the simulation. Context is the specific time range that researchers are interested in modeling, for example, situations in the morning, afternoon, and evening.

(2) **Simulation Phase***:* the researcher to specify which context to simulate. Each context has the default state of the sensor and position of the participant. Then the participants started to simulate their ADL in this situation. During the simulation, the sensor output and the status of various devices are recorded and saved in a temporary data set. The modeling or simulation phase aims to capture the details of the actual interaction between participants.

(3) **Aggregation Phase**: the researcher can aggregate the participants' generated sample activities i.e. Create the final recorded event. The result of the modeling phase forms a series of typical actions for each context.
The aggregation stage aims to provide a solution for generating large data sets in a short modeling time. Therefore, in this paper, an algorithm developed to reproduce the results of the simulation phase by extracting enough samples for each expected context. This feature allows OpenSHS to combine the advantages of both approaches, a hybrid approach.
   1) Events Replication: development of this work is not feasible for a participant to sit down and simulate his/her ADLs for a whole day and want to record the interaction between residents and SH. These requirements brought up the concept of real-time context simulations that the user simulates only a specific context, not all day. The replication algorithm used to expand and expand the data set selection is proposed in [20].
   2) Dataset Generation: combine all actions generated into one final dataset output.

B. OpenSHS Implementation

OpenSHS depend on game engine of on Blender with Python editors [9].

(1) **Blender***:* Blender was chosen to build the simulation tool for these reasons:
   1) *Open-source:* game engine enables users to create complex interactive 3D games and Python scripts.
   2) *Cross-platform:* Blender is available for all three major operating systems. Namely, GNU/Linux, Microsoft Windows, and Japanese Apple macOS. Blender uses OpenGL for its Game Engine which is also, a cross-platform 3D technology available for the major operating systems.
   3) *The Blender Game Engine:* The physics engine facilitates the simulation of different types of real sensors and devices. For example, Blender has a (Near) sensor that only triggers when the user-controlled 3D avatar is physically close to other objects in the scene.

(2) ***Python****:* All logic and interactions between the avatar and the virtual environment are developed with it. In addition, all OpenSHS modules are programmed in Python.

C. The proposed approach

OpenSHS simulator turned into used for dataset generation. SH turned into designed, sensors turned into reading and a data set turned into generated. Normally simulation scenes can only be handiest be managed through the Blender GUI. It turned into progressed to remotely manage gadgets through a steady HTTP server with a REST API that don't permit unauthorized customers to get entry to the server. A running HTTP server with Blender scene and client were built with jQuery. WebOb used python library to provide objects for HTTP requests and responses by wrapping the WSGI request surroundings.

Two sensors have been assigned, each with one controller for any Object in simulation scene that needs to be controlled. The first sensor is attached to a controller which runs a feature of a Python module to initialize the threading controller once. A 2nd sensor runs feature of a Python module for managing the messages originating from the internet customer and begins the HTTP server on port 8000.

The flow chart for the proposed approach is presented in figure 1. The Design phase and simulation phase is presented in figure 2. The secure control HTTP server is presented in figure 3.

The steps of the proposed approach: The first step contains design floor plan, import smart devices; assign activity labels. Then SH started by loading the SH context file by following these commands (cd app/, press enter, python openshs start -c evening, press enter, click on P) this will starts a blender session with the evening context simulation. Second step:

simulation phase that contains design context, and starting the secure control HTTP server that begins password, Html web page to prevent unauthorized users. In case of an incorrect password, the user will be prevented from reentering password for one minute. In case of a correct password the user can open the server and retrieve information on all objects in the SH simulation scene and change their properties. All the interactions saved into datasets that leads to the final step Aggregation phase contains read sensors for validation.

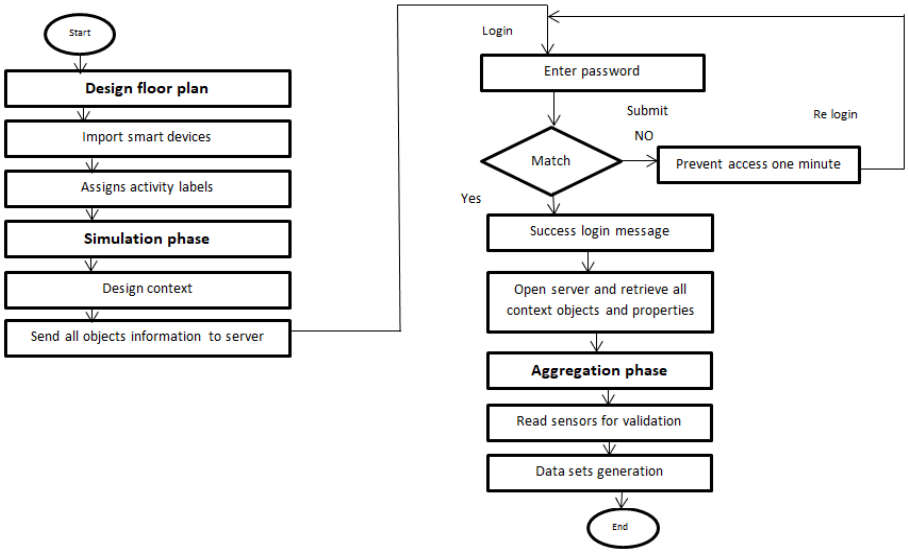

Fig. 1. The proposed approach folwchart.

Fig. 2. The Design phase and simulation phase.

Fig. 3. The secure control HTTP server.

IV. EXPERIMENTAL RESULTS

In this section, firstly the Experimental setup for control HTTP server was introduced. Secondly, security model evaluation was introduced with different four passwords within their success rate. Thirdly, confusion matrix for the most secure password is presented.

(A) **The experimental setup for control HTTP server***:* . The experimental setup of the Html web page preventing unauthorized users has two cases. In case of an incorrect password, the user will be prevented from reentering password for one minute. In case of a correct password the user can open the server and retrieve information on all objects in the SH simulation scene and change their properties. The success login was presented in figure 4. The login with wrong password and wait one minute message was presented in figure 5.

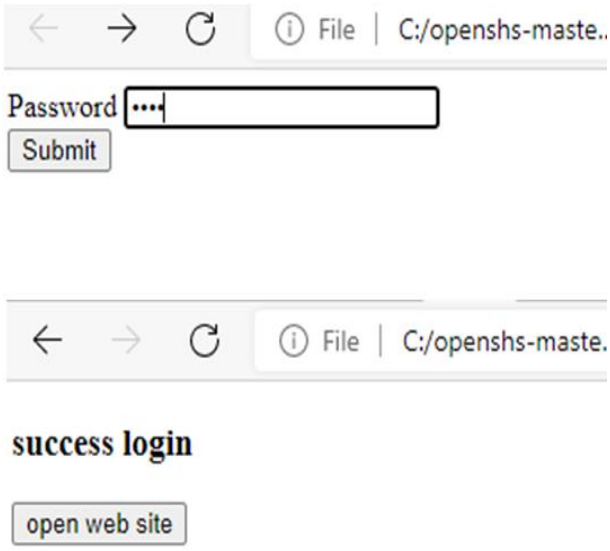

Fig. 4. Login with correct password.

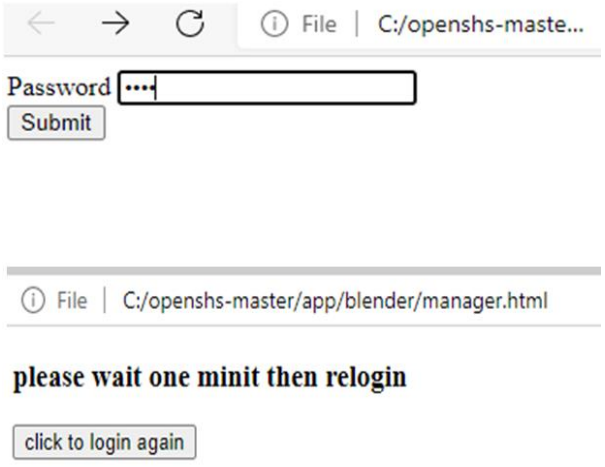

Fig. 5. login with wrong password and wait one minute message.

(B) **The success rate for four passwords:**

The success rate for the different four passwords is shown in table 1the (1234) password has the higher success rate of 96%, (1111) has 79%, (1356) has 92% and (1221) has 87%.
As can be seen in Table 1, the success for passwords with different button numbers has the highest success rate, which is 96%.
The password that has the same button number has the lower. However, this result will depend on other variables as well such as the speed of pressing the button, the time duration of the button being held down when being pressed and others. This means other users will have a different success rate. Based on these results (1111) password is the most secure because the password has the lowest success rate on entering it so it was selected for proposed approach. Figure 6 shows the success rate for four passwords.

(C) **Evaluation by confusion matrix for (1111) password:**

The purpose of the authorization is to control the authenticated entity's access rights to network services and resources. The confusion matrix is a predictive analysis tool.
The confusion matrix generates indicators of metrics such as accuracy, precision.
A false negative: when user is not having access is prevented from access to the system.
A false positive: a user who is prevented from access is having access to the system.
A true negative: when user have access is have access in the system.
A true positive: Users who not have access is prevented to access in the system.
Table 2 shows the confusion matrix.
Error Rate is how often is it wrong?
Error Rate (FP+FN)/total = (0+0)/100 = 0.
Accuracy is the division of correctly predicted by the total.
Accuracy = (TP+TN) / (TP + TN+FP +FN) = (266+734) / (1000) = 1.
Precision is division of correct positive to the total predicted positives.
Precision = TP / (TP + FP) = 266/266 = 1.
A recall is the division of correct positive to the total positives.
Recall = TP / (TP + FN) = 266/266 = 1.
F-Measure provide you way to collect precision and memory in one dimension while getting both values.
F-Measure = (2 * Precision * Recall) / (Precision + Recall) = (2*1*1)/2 = 1.
Table 3 shows the confusion matrix for (1111) has results that Error Rate=0. Precision = 1, Recall = 1, Accuracy = 1, F-Measure = 1.

TABLE 1. The success rate for four passwords

Password Test	Trials	Success trails	Fail trails	Percentage of error (%)
1234	200	192	8	0.08
1111	200	159	41	0.41
1356	200	184	16	0.16
1221	200	174	26	0.26

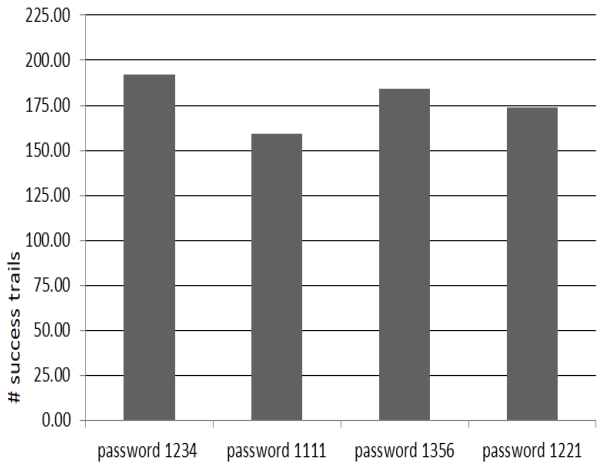

Fig. 6. The success rate for four passwords

TABLE 2.cofusion matrix

Trail numbers	Predicted Normal	Predicted Attacks
Actual Normal	TN	FP
Actual Attacks	FN	TP

TABLE 3.cofusion matrix for "1111"

N=1000	Predicted Normal	Predicted Attacks
Actual Normal	734	0
Actual Attacks	0	266

V. CONCLUSION

Access to sensor data sets needed to test new methods of data analysis. However, due to high cost and design, the availability of such data sets is limited. By using data modeling methods, researchers can address these limitations, providing researchers with rich datasets to test new data analysis methods, especially in the early stages of development. In this paper, OpenSHS used as a hybrid SH simulator to generate dataset. Firstly a SH was designed with (OpenSHS) tool. Secondly a data set was generated by SH simulation for training, testing, and validating. Thirdly sensors reading collected for validation of the SH. OpenSHS was improved to be controlled remotely by the HTTP server. This means that with this web service it is possible to retrieve information on all objects in the SH and changes their properties remotely. A security model was developed for protecting SH from unauthorized users by design a simple login webpage with a password. Finally, security model was evaluated with accuracy of the password with its success rates for different passwords then the confusion matrix was calculated for the most secure password.

In the future, we will make our approach have more control on objects of SH simulation. We will also perform other testing type like performance test and functional test for the proposed system.

REFERENCES

[1] S.Pallavi, and R.Sarangi, "Internet of things: architectures, protocols, and applications" , In Journal of Electrical and Computer Engineering, 2017.

[2] T.Muheidat, and F.Tawalbeh, "IoT Privacy and security: Challenges and solutions" , Applied Sciences, vol. 10(12), pp.4102, 2020.

[3] D.Menachem, "Smart home systems based on internet of things", Internet of Things (IoT) for Automated and Smart Applications, 2019.

[4] G. Punit, and J.Chhabra, "IoT based Smart Home design using power and security management" In the International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), IEEE, pp. 6-10, 2016.

[5] B.Mario, W. Kurschl, and J.Küng, "A simulator for generating and visualizing sensor data for ambient intelligence environments", Procedia Computer Science, pp.90-97, 2011.

[6] V.Andrei, I.Andrei, A.Silvia, and N.Goga, "Smart home simulation system", In 2016 IEEE International Symposium on Systems Engineering (ISSE), IEEE, pp. 1-5, 2016.

[7] V.Andrei, and B.Bernovici, "Lightweight smart home simulation system for home monitoring using software agents", Procedia computer science 138, pp. 153-160, 2018.

[8] K.Howard, "Simulating IoT Frameworks and Devices in the Smart Home" , PhD diss, Virginia Tech, 2017.

[9] A.Asma, and C.Perera, "Smart Home Human Activity Simulation Tool for OpenHab-based Research" , In Technical Report, ACM, 2019.

[10] A.Nasser, T.Alshammari, M.Sedky, J.Champion, and C.Bauer, "Openshs: Open smart home simulator", Sensors, vol. 17(5), pp.1003, 2017.

[11] S.Jonathan, C.Nugent, and P.Jeffers, "Simulation of smart home activity datasets" , Sensors, vol. 15(6), pp. 14162-14179 , 2015.

[12] Blender. http://www.blender.org , accessed on 06 November 2016.

[13] I.Laura , "The smart home as a place of control and security: an analysis of domestication of smart technologies for the making of a home" , PhD diss , Université de Neuchâtel, 2017.

[14] J., P., and Y.REDDY, "Home Security System Based on Face Recognition Web-Based Online Door Control System", In the International Journal of Scientific Engineering and Technology Recearch, Vol. 06(18) , pp.3597-3599 , 2017.

[15] H.Brandon, D.Vogts, and J. Wesson, "A smart home simulation tool to support the recognition of activities of daily living" , Proceedings of the South African Institute of Computer Scientists and Information Technologists, pp. 1-10 ,2019.

[16] T.Surya, I.Yaldi, M.Kartiwi, and H.Mansor, "Performance evaluation of smart home system using internet of things" ,International Journal of Electrical and Computer Engineering, vol. 8(1), pp. 400, 2018.

[17] B., K., A.Ajroud, B. Bouchard, and A. Bouzouane, "SIMACT: A 3D open source smart home simulator for activity recognition with open database and visual editor" Int. J. Hybrid Inf. Technol vol. 5(3),pp. 13-32, 2012.

[18] H., A., K. Cho, W.Lee, Y. Sung, J. Lee, and E.Kim, "3D modeling and simulation of human activities in smart spaces" , In 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, pp. 112-119. IEEE, 2012.

[19] R., B., and B.Vigário, "HOME I/O and FACTORY I/O: a virtual house and a virtual plant for control education," IFAC-PapersOnLine, vol. 50(1),pp. 9144-9149,2007.

[20] A.Nasser,T.Alshammari, M.Sedky, J.Champion, and C.Bauer, openshs/openshs: First alpha release. https://doi.org/10.5281/zenodo.274214 , 2017.