Journal of Theoretical and Applied Information Technology
30th November 2020. Vol.98. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SENSING PERFORMANCE ANALYSIS OF AN INTERNET OF THINGS-BASED INTRUDER DETECTION SYSTEM

ARKOM SUDRAM[1] , WASANA BOONSONG[2]

[1]Department of Mechatronic Engineering, Faculty of Industrial Education and Technology, Rajamangala University of Technology Srivijaya, Songkhla 90000, Thailand
[2]Department of Electronic and Telecommunication Engineering, Faculty of Industrial Education and Technology, Rajamangala University of Technology Srivijaya, Songkhla 90000, Thailand

E-mail: [1]sudram18@rmutsv.ac.th, [2]wasana.b@rmutsv.ac.th

ABSTRACT

The Internet of Things (IoT) has become part of human life since it has made interconnection among people and things together. IoT impacts a security because affected an individual's well-being. This paper contributes a performance analysis of an intruder detection system based on IoT service network platform. The IoT cycle of intruder monitoring/detection system considered are consists of 4 sections, which are 1) intruder monitoring section, 2) communication network, 3) data processing unit and 4) user interface. Each section has its different role but they work together seamlessly and efficiently. The proposed intruder monitoring device system adopted the Ultrasonic and Passive Infrared (PIR) Sensors. Both were tested the moving detection accuracy performance with various distances in detecting a moving object. The findings were analyzed in terms of percentages. NETPIE-IoT cloud server acts as an intermediary to exchange information with other devices on the internet network. The statistical package for the social sciences (SPSS) used for analyzing the experimental results by comparison between the two their performances. The results showed that the Ultrasonic and PIR sensors show different responses based on individual tests. Both intruder sensors have a statistically significant differences in percentages of moving detection accuracy with 99.94 (Std. Deviation = 0.113) and 99.56 (Std. Deviation = 0 .679) respectively. The Ultrasonic sensor was slowly dropped, whilst the PIR sensor was slightly increased according the distance variations.

Keywords: *IoT, Ultrasonic, PIR, NETPIE, SPSS*

1. INTRODUCTION

The Internet of Things (IoT) is actively shaping both the industrial and consumer worlds. Smart technology has found its way into every business and consumer domain, such as healthcare, logistics, transportation, etc. in which a big opportunity strategically employed by a company can easily qualify as a long-term failure for companies who do not innovate.

With the IoT there is an interesting concept regarding network communication among things in that they can interconnect with one another through wirelessly embedded sensor devices. In this paper, the performance of an intruder detection system based on IoT network service platform is investigated; this focuses on the performances of moving detection accuracy of sensor devices. The system being considered includes the following components: 1) intruder monitoring device, 2) communication network, 3) data processing unit and 4) user interface. The cycle of the proposed intruder detection system is as shown in Figure 1.

Journal of Theoretical and Applied Information Technology
30th November 2020. Vol.98. No 22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

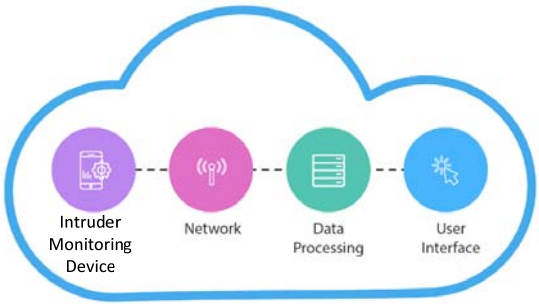

Figure 1: IoT Cycle of The Proposed Intruder Monitoring System Application

1. Intruder monitoring device: The multiple intruder sensors gather the sensing information at the point of restricted monitoring area. The Ultrasonic and Passive Infrared (PIR) sensors are adopted to sense the biological, environmental, visual, auditory, or any combination of these.

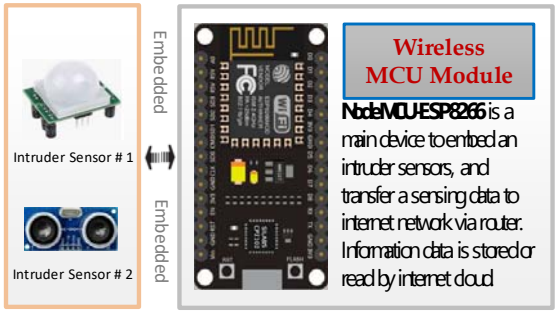

Figure 2: Proposed Embedded Monitoring Module

Figure 2 presents the embedded design of the intruder sensing and wireless NodeMCU module by using the concepts of automation and control with optimized resource consumption. Namely, the wireless sensor network and the automatic answering sensor which can assist to analyze the safety monitoring appropriately.

2. Communication: A communication channel uses wireless sensor network and IoT, but sometimes need cellular network with short-range capabilities, such as Bluetooth, Z-wave or ZigBee which are the near field communication devices to transfer the monitored information data to a storage on an internet cloud server. Whichever, the network communication depends on the suitability of factors in selecting the particular service, such as low power consumption, low cost and maintenance service, etc.

3. Data storage and consolidation managements: This part is about data storage and analysis before making decision for data management in the next step. The IoT information from the all intruder sensing devices were gathered and generally communicated to a cloud-based storage space. The raw data needs to be processed along with other sources to extract the useful information. Therefore, for all detecting sensors – driven decision analytics, the IoT can take advantage of complex long-term planning and decision making, in which this part may be a disadvantage of the system. Real issue with this application is that it actually requires a large amount of space for data storage and also an updated software system that can display graphic data for analysis, such as accurate positioning which will assist in gaining the safety of life and property by using the smart IoT platform.

4. Information portal: the information portal is the end user of the procedure, such as consumer, commercial user or just a machine. The user obtains the information through a portal that usually offers analytical insights. Thus, the wireless NodeMCU-ESP8266 was connected to the selected intruder sensors. The information was transmitted to the user at a host station.

Meanwhile, advances in the technology of Internet of Things (IoT) have led to significant progress in the application of environmental tele-monitoring. In the area of aquatic monitoring and wireless transmission have been widely designed by the research institutes [6, 7] or deployed by environment departments [8], and so on.

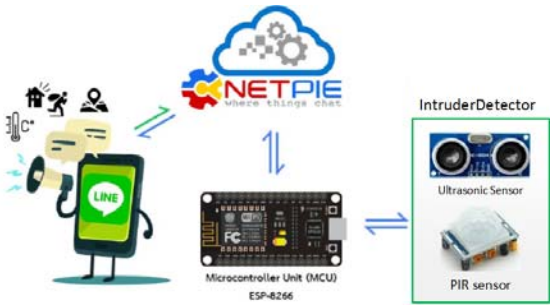

Figure 3: Proposed Intruder Detection System

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 3 shows the proposed intruder detection system. The data from those sensors can inform the detecting environment of its condition. In order to improve a decision-making efficiency, for example, security systems use sensor networks that include warning messages, and alarm detectors to point out people who have been restricted from an area.

2. Wireless Communication Technology

The proposed IoT innovation system, the intruder sensing devices will be connected to the wireless sensor network for two-way data sources, which is called machine-to-machine (M2M) communication. The wireless communication technologies are used as following applications.

2.1 Wireless Communication for IoT Application

In the present time, there are various wireless connection and communication technologies between IoT devices. Each model has different standard features in terms of radius and the speed of data transmission (throughput). However, the authors would like to divide the wireless connection technology as follows.

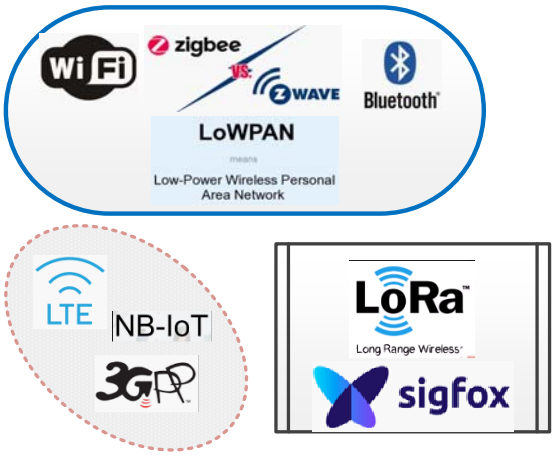

Figure 4: Types of Wireless Communication Technology

Figure 4 presents the group of wireless communication technology, which they are 3 main types. The advances in low power wireless technology is the major consideration. Several wireless technologies in the group of low power wireless personal area network, such as Bluetooth low energy, IEEE 802.15.4, ZigBee, Ultra-Wide Band (UWB) and Radio Frequency Identification (RFID) [1] could be used to implement a wireless sensor network (WSN) to overcome the problems related to the propagation of the electromagnetic wave through the structure and for node autonomy.

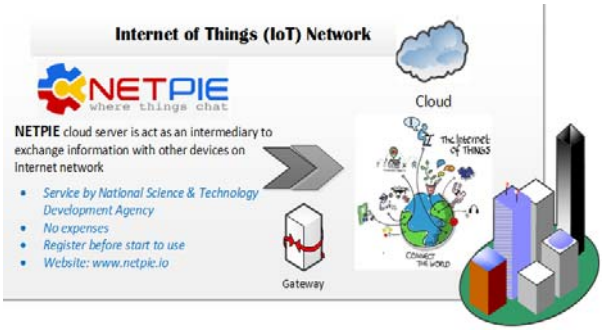

Figure 5: NETPIE Communication through the Internet of Things (IoT) Network

Figure 5 shows the NETPIE application on Internet of Things (IoT) or Internet of Everything (IoE) cloud-based platform. IoE is a term used to refer to the interconnection of everything in our daily life, which includes computer, tablet, smart phone, etc. Moreover it also refers to the electronic devices used, such as smart TV, or other smart devices that apply RFID technology and Near Field Communication (NFC). NFC is a wireless data communication technology using frequencies within a distance of 10 centimeters. It can transmit data via touch and read, consume low power and can be used with other devices without electricity. In this work, NETPIE was adopted to work as an IoT cloud platform as a service that helps connect the embedded IoT devices together seamlessly by pushing the complexity from the hands of application developers or device manufacturers to the cloud.

2.2 Why NETPIE

The NETPIE IoT platform was provided for Thai developers and industries, aims to be a first platform to connect devices or tools. The first phase focuses on supporting developers and small industries (SMEs) to build capacity and strength for the large Thai industry of Thailand. As the government has announced the vision of Thailand 2015-2020 of **"STABLE, WEALTHY and**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENDURE" with the goal of increasing the country's competitiveness to liberate from middle income countries. The National Electronics and Computer Technology Centre (NECTEC) considers that the innovation economy is the important mechanism for the country to be the basis for other mechanisms in all sectors to achieve the GOAL [2]. Some of the reasons for employing NETPIE IoT platform include:

- **Reduction in the resources of connection:** It is able to connect all devices to one another with remote access capability, which is responsible for connecting all devices together even if they are different network companies. Moreover, it assists in getting started easily, and it can plug and play with automatic discovery.
- **Reduction in the burden of data security:** the intruder notifying system is designed to have right access at the Fine Grain level; namely, users can design for talking, reading or writing information. In case a user requires to un-use, it can be revoked under any conditions.
- **Flexibility in expanding the system:** the proposed NETPIE is truly a cloud server architecture in all system components with flexibility and high mobility in expansion. Each module is designed to work separately and to communicate with one other using asynchronous messaging method with highly reliable platform, which is easy to use and develop [3].

Figure 6: Advantages of NETPIE Application

Figure 6 presents the advantages of NETPIE application, which are totally fee, highly scalable and commercial ready. NETPIE is free forever, no trial-period, no expiration, the free quota is replenished monthly. It is a new micro-service architecture that enables maximum scalability and fault-tolerance. Furthermore, NETPIE is free to use for commercial purposes. Migration to the commercial platform is smooth and seamless.

2.3 NETPIE for Smart Office

Since the public release of the first phase for the NETPIE (Network Platform for Internet of Everything) research on 16th September, 2015 by NECTEC-NSTDA development team, it aimed to set an initial goal of providing services and encouraging Thai developers and small industries (SMEs) a platform to interconnect Internet of Things (IoT) devices. The latest utilization version of the NETPIE has grown steadily for both educational and economic purposes to support a wide variety of the IoT applications with greater flexibility to meet the needs of a growing number of commercial users, especially the industrial sector under the newly designed architecture with many additional features. Namely, it will reduce the burden on users and become easy from the prototype creation process up to the system development for commercial use, including maintenance. [NSTDA = National Science and Technology Development Agency, an agency of the Thailand Government]

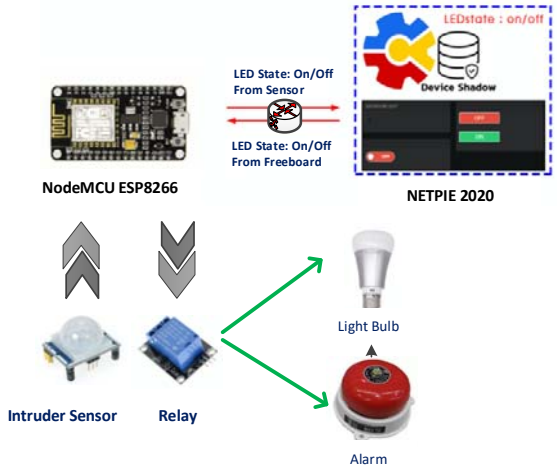

Figure 7: NETPIE Application for Smart Office-Based Intruder Alarm System

Figure 7 presents the NETPIE 2020 applied for the smart office-based intruder alarm system with newly designed architecture and many existing new features. The proposed IoT works on NETPIE capability to connect with NodeMCU-ESP8266 hardware and the intruder sensor

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

platforms and applications regardless of computer languages involved. The proposed intruder detection system with authorization management in which users can conveniently and dynamically add, drop and group their authorized devices based on their requirements. This feature is very powerful for the users that build the IoT products for third-party use. The sensed data for each device on the network will be stored in a virtual database at the latest status and real-time monitoring.

In addition, LINE API is also provided to service called LINE Notify that can send information messages or alarm to the LINE application on smart phone. The LINE APP service used is a common HTTP POST by accessing token is applied as a code when requesting the LINE API [4]

2.4 LINE Application Programming Interface

The proposed intruder detection system adopted LINE the application programming interface (API) for receiving a warning data from an end device module. The API requires "Code" to allow software programs to communicate with each other, and it is a method for requesting commands from operation system (OS) or other applications.

Figure 8: Messaging API on LINE API

The messaging API adapted with the intruder detection system, which it always allows an end device sensor to send information data between servers to user LINE through LINE platform as shown the structure in Figure 9.

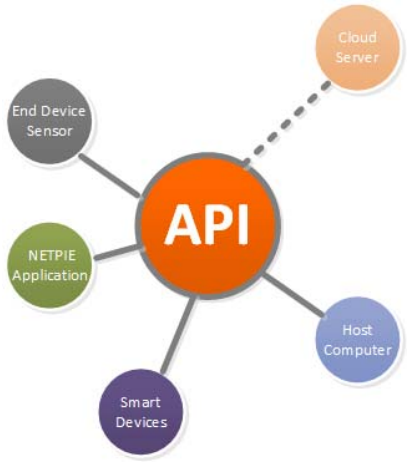

Figure 9: API as communication center for multi-device

The REQUEST for sending data must be in JSON format. APIs are made up of two important parts: 1) a specification that describes the exchange of data between programs, which are documented to indicate request/response 2) software written according to the specification and spread it out for use. The receiving data from LINE Platform, the information will be sent to the URL of server wherever there is a user contacting account, which are 1) user sends a message (message) 2) user has actions such as add our LINE ID as a friend (operation).

Usually, the applications with APIs will be written by using *C* programming language, which is easy to develop. Therefore, it is necessary to inspect and test the structure of the API.

3. Experimental Results and Discussions

The performance test of the intruder detection system on IoT platform is considered. The results are presented in the following subsections.

3.1 The Access Point and Web Server Test

The experiments on the access point and the web server test are mentioned in this section. More details on the installation setup and NodeMCU-ESP8266 use as an access point and web server will be discussed. That is, NodeMCU-ESP8266 used as an access point and web server to support the connection of clients by mobile devices, smart phones, tablets, computers and others.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Moreover, it (the node) can send the request signal to open the web page without the requirement of an external access point devices because its mainboard already supports being an access point and a web server. Therefore, it is easy to use and not complicated as real computers and can support connection to more than one client.

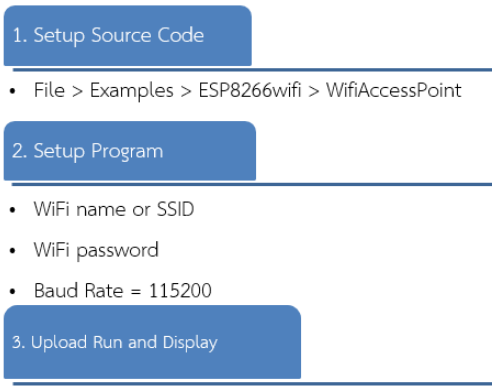

Figure 10: The Procedures of NodeMCU, Client and Website Connection

Figure 10 shows the step of procedures of NodeMCU WiFi module, client and website communication. The wireless NodeMCU ESP8266 can communicate with client devices effectively through access points and it acts as web server and as a WiFi spreader, eliminating the need for external WiFi signal. From the experiment using a computer or smart phone as a client, connect to the access point with same WiFi band and open the web by inserting the IP as shown in the Serial Monitor Figure 11.

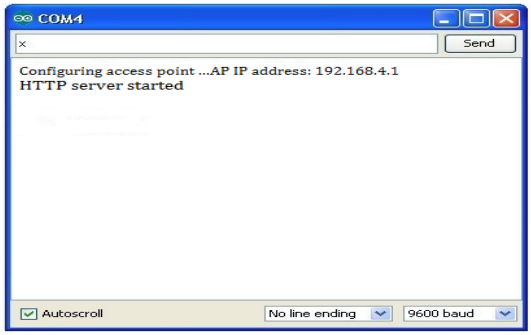

Figure 11: The Connection Test Results to Access Point on Serial Monitor

Moreover, from the study of "wireless intruder detection system through mobile phone" is verified the performance of the accuracy of detection system is verified as in section 3.2.

3.2 The Performance Tests of Intrusion Sensors

Generally, the intrusion detection system consists of exterior and interior intrusion sensors, a video alarm assessment, entry control and alarm communication systems all working together. Exterior sensors are those used in an outdoor environment, and interior sensors are those used inside the buildings. In this study, the intrusion detection is defined as the detection of a person attempting to gain unauthorized entry into an area that is being protected. The intrusion detection boundary is ideally a sphere enclosing the item being protected so that all intrusions, whether by surface, air, underwater or underground are detected [5]. The development of intrusion detection technology has emphasized detection on or slightly above the ground surface with increasing emphasis being placed on airborne intrusion. Thus, this session primarily covers ground-level perimeter intrusion detection systems. Thus, both types were adopted to test and compare their performances in this study.

Intruder sensors are typically incorporate a short delay prior to generating an alarm, in order to allow an authorized person to deactivate the system without sending a false alarm to the monitoring station. Types of intrusion sensors include of magnetic contact switches, glass break sensors, motion sensors, electric eye, seismic sensors, pressure sensors. This experiment, the Ultrasonic was adopted because it has greater accuracy than many other methods at measuring thickness and distance to a parallel surface. While, the PIR sensor was detecting sensor uses heat emitted to detect place of an object or a living creature.

The system investigated in this work consists of the hardware and software. The Ultrasonic and PIR sensor devices are tested for their accuracies in terms of percentages. The comparison of both sensing devices are analyzed as plotted in Figure 12.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

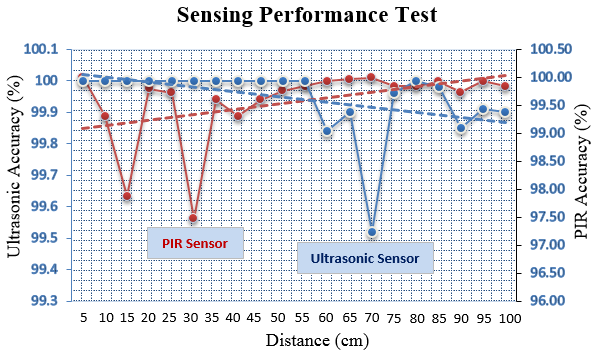

Figure 12: Comparison of Ultrasonic and PIR Sensing Performances

Graph in the Figure 12 compares the performances of the Ultrasonic and PIR sensors. It was found that the Ultrasonic sensor was slowly dropped, whilst the PIR sensor was slightly increased according the distance variations. Both sensors have a different application characteristic. First, Ultrasonic sensor was tested and its characteristic was also discussed. The Ultrasonic sensing concept based on the amount of current was recorded by the IC across the plates. In the zero intrusion state, let the current recorded across the plates be I amperes and in case of any intrusion let it be I_R [6] as described by the equation (1).

$$I = I_R + I_H \quad (1)$$

Whenever, any manner of interference is encountered by intrusion in the defined boundaries of the electric field. The disturbance creates a change in the feedback of current as shown in Figure 13.

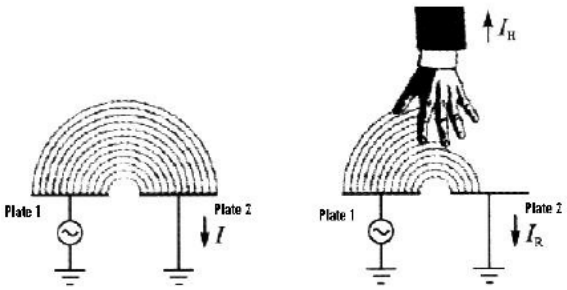

Figure 13: Visual Explanation of Ultrasonic Electrode Current

Figure 11 shows the concept of active ultrasonic sensors. Actually, they are motion detecting devices that work similar to radar and sonar utilizing the Doppler principle [7, 8]. They emit ultrasonic sound energy into a monitored area and reacts to a change in the reflected energy pattern. Based on the individual experiment, the ultrasonic sensor was installed and placed typically on a ceiling. Thus, it can be used together with passive infrared (PIR) sensor to provide a greater probability of detection. Because these sensors are dependent upon reflections, or echoes from a moving intruder, clear line of sight between the sensor and the intruder are required so that energy can be transmitted to the intruder and reflected without obstructions in the way.

Based on the experiment, the Ultrasonic sensor is not affected from changes in the thermal environment. It only can detect motion even behind partial obstructions. The key advantage of the ultrasonic sensor is about its ability to calculate the distance to the object in motion exactly [9]. However, the effectiveness of the Ultrasonic sensor also depends on the user's calibration.

On the other hand, the Passive Infrared Sensors (PIR) are passive, visible, and volumetric. This sensor responses to change in the energy emitted by a human intruder, which is approximately equal to the heat from a 50-W light bulb. Infrared electromagnetic radiation is outside of the visible light spectrum and is emitted by all living beings and surrounding objects which can also be thought as radiated heat. Instead, they are only detecting the reflected heat from objects which are moving in their detracting range [9]. Namely, they also detect changes in the background thermal energy caused by someone moving through the detector field of view and shadowing the energy emanating from the objects in the background. The Infrared Radiation (IR) is tested based on the following characteristics:

1) IR is emitted by all objects and it is related to the object's temperature.

2) IR energy is transmitted without physical contact between the emitting and receiving surfaces.

3) IR warms the receiving surface and can be detected by any device capable of sensing a change in temperature.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4) IR is invisible to the human eye, thus PIR sensors respond to infrared energy in the wavelength between 7 and 14 nm.

The PIR sensor is applied depending on the optics installed, which are suitable for exterior (outdoor) and interior (indoor) surveillance. Based on the elements inside, PIR detectors can cause shadows, which prevent detection or give rise to false alarms. Based on the experiment this sensor is sensitive to weather. That is, when body temperature and ambient temperature are similar, the PIR sensor cannot detect. However, when there is a sudden temperature change such as air turbulence or exhaust from devices, this can create a moving object response which can activate false alarms, which is consistent with G. Yatman [10].

3.3 Data Analysis Related

In this section, the obtained results from PIR and Ultrasonic sensors are analyzed by using the independent-sample *t* test statistic. The *t* test evaluates the difference between the averages of two independent variables, which unrelated to each other. The hypothesis of the study was expected that the analyzed results are significantly different based on their sensing characteristics. The independent-samples *t*-test is commonly referred to as a between-groups test and design.

The assumptions underlying the independent-samples *t*-test:

1. The data (obtained results) are independent of each other. This is commonly referred to as the assumption of independence.
2. The test (dependent) variable is normally distributed within each of the two results. This is commonly referred to as the assumption of normality
3. The variances of the test (dependent) variable in the two populations are equal. This is commonly referred to as the assumptions of homogeneity of variance.

Thus, the null hypothesis (H_0) and alternative hypothesis (H_1) of the independent sample *t*-Test can be expressed in two different but equivalent ways:

H_0: $t_1 = t_2$ (the two result test means are equal)
H_1: $t_1 \neq t_2$ (the two result test means are not equal)

Table 1: The obtained test results from different two sensors

No. of Test	Types of Sensor	
	Ultrasonic	PIR
1	100.00	0.00
2	100.00	99.30
3	100.00	97.87
4	100.00	99.80
5	100.00	99.72
6	100.00	97.47
7	100.00	99.60
8	100.00	99.30
9	100.00	99.60
10	100.00	99.76
11	100.00	99.84
12	99.84	99.93
13	99.90	99.97
14	99.52	99.99
15	99.96	99.84
16	100.00	99.84
17	99.98	99.92
18	99.85	99.73
19	99.91	99.93
20	99.90	99.84

3.4 Analysis of the Sensing Performances

This experimental results in this Section gives the analysis of the sensing performances in term of mean, standard deviation, and standard error mean values for both Ultrasonic and PIR sensors. The results are tabulated in Table 2.

Table 2: Comparison of average reliability values for moving detection between Ultrasonic and PIR sensors using the SPSS program

Group Statistics

	type	N	Mean	Std. Deviation	Std. Error Mean
Sensors	Ultrasonic	20	99.9430	.11323	.02532
	PIR	20	99.5625	.67971	.15199

Table 2 summarizes the mean, standard deviation, and standard error mean comparisons of measurement accuracy for object detection performance between the Ultrasonic and PIR sensors. The results are analyzed by using SPSS program to clarify the performance in terms of the detection accuracy versus the various distance tests of both sensors. It was found that the average reliability value of moving detection of the Ultrasonic and PIR sensors are 99.94 %, and 99.56 % respectively. Moreover, the standard deviation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for the Ultrasonic and PIR sensors are 0.113 and 0.679 respectively.

The comparison results based on individual test in Table 2, show that the variance of the F-value is .004, which is less than .05 at the reliability of 95 %. Therefore, the P Sig. (2-tailed) of this test is .023. Based on the Independent Sample statistic tested [11] for the detection accuracy of the Ultrasonic and PIR sensors, it can be summarized that both types of moving detection sensors have significantly different performances at a reliability test level of 95 %.

The statistical tool used to analyze the experimental results is SPSS because it's used by various kinds of researchers for complex statistical data analysis. It is the set of software programs that are combined together in a single package. Usually, the basic application of this program is to analyze scientific data related with the social science, which can be used for market research, surveys, data mining, etc. With the useful of the obtained statistical information, authors can easily to understand the conclusion of any experiment. Thus, that is all the reason these obtained result were analyzed using SPSS program as well.

Table 3. The accuracy difference tests of Ultrasonic and PIR sensors using Independent Sample t-Test statistic

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Sensors	Equal variances assumed	9.328	.004	2.469	38	.018	.38050	.15408	.06858	.69242
	Equal variances not assumed			2.469	20.054	.023	.38050	.15408	.05914	.70186

Table 3 proofs the difference mean between the results from Ultrasonic and PIR sensors using Independent Sample *t*-Test. The Independent Sample *t*-Test or called unpaired sample *t* test is the most common. This type of statistic helps you to compare the means of two sets of data, which is depending on the sources of data selected. In this case, the data collected are two main types of sensors, thus the paired *t* test (dependent samples) are used to analyze the related experiments.

In the beginning, the authors have made assumption that the two intruder sensors are significantly different in term of sensing performance. Then, the procedures are conducted to receive the conclusion results using Independent Samples *t*-Test. The statistic is used to confirm the reliability of results calculation. The assumptions for the Independent Samples *t*-Test, which is come out according to the graph in Table 3. Both sensors which ultrasonic and PIR sensors are the motion detection, but the ultrasonic sensor is more flexible and can be used in a variety of uses. Hence, these information in this research article will be useful for those who require to use both types of devices.

4. Conclusion

Security and privacy are considered key issues in any real-world smart environment based on IoT model. This work applies on the IoT intruder detection system sending data through LineBot using NETPIE platform.

The access point and web server setup was successfully tested on NodeMCU-ESP8266, which was connected with smart phone as well as possible depending on the connection's quality. Moreover, it is about the network service density.

The performance analysis based on moving detection was tested for both sensors, such as Ultrasonic and PIR Sensors. The reliability of accuracy test is analyzed in term of percentage. That is, the reliability results of both sensors came from the accuracy of their moving detection based on the individual test on IoT communication platform. The results were analyzed using SPSS program. It was came out with slightly difference in terms of percentage moving detection significantly

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of 95 % confidence level. This is because the sensing network system needs to be developed for the optimum security system required by selecting the suitable sensors and subsystem components according to the environmental conditions for the restricted area. Besides being used in security applications, the smart sensor systems could be installed to monitor activities in our daily life using wireless sensor networks and the IoT platform. It is to track the sensed information and remotely send to the users through smart devices with real-time monitoring.

ACKNOWLEDGEMENT

The authors are grateful to Rajamangala University of Technology Srivijaya Songkhla, Thailand for the research grant for sponsoring the development of the in-house built-in devices in the fiscal year 2019 (Grant No. 669).

REFRENCES:

[1] J. Cabezas., T. Sanchez-Rodriguez., J. A. Gomez-Galan., H. Cifuentes and R. G. Carvajal, "Compact Embedded Wireless Sensor-Based monitoring of Concrete Curing," *Sensors (Basel)*, 2018, pp. 1-17.

[2] National Electronics and Computer Technology Center (NECTEC), "NETPIE," [online], [Accessed 28 February 2020]. Available from World Wide Web: https://netpie.io/about

[3] W. Boonsong, "Smart Intruder Notifying System Using NETPIE through Line Bot Based on Internet of Things Platform", 2019 *IEEE 5th International Conference on Computer and Communication*, 2019, pp. 2208-2211.

[4] E. Boonchieng., O. Chieochan and A. Saokaew, "Smart Farm: Applying the Use of NodeMCU, IOT, NETPIE and LINE API for a Lingzhi Mushroom Farm in Thailand", *2018 The Institute of Electronics, Information and Communication Engineers*, 2018, pp. 16-23.

[5] J. Cabezas., T. Sanchez-Rodriguez., J. A. Gomez-Galan., H. Cifuentes and R. G. Carvajal, "Compact Embedded Wireless Sensor-Based Monitoring of Concrete Curing", *Sensors*, 18(3), 2018, pp. 1-17.

[6] R. Sharma., K. S. Dhingra., N. Pandey., R. Garg and R. Singhal, " Electric Field and Ultrasonic Sensor Based Security System," *2010 International Conference on Intelligent System, Modelling and Simulation*, 2010, pp. 423-426.

[7] T. S. Khye., N. C. Sim and S. S. H. You, "Comparative Analysis of Radar and Sonar Principles", *DSTA HORIZONS*, 2011, pp. 91-98.

[8] Y. Ji., J. Zhan., Y. Wang., X. Chu and M. Li, "Vessel target detection using zero-Doppler spectra of radar echo for high-frequency surface wave radar", *Journals IET Radar, Sonar & Navigation*, 2016, pp. 1-7.

[9] L. Hodges, "Ultrasonic and Passive Infrared Sensor Integration for Dual Technology User Detection Sensors", *Michigan State University*, 2009, pp. 5-6,.

[10] G. Yatman, S. Uzumcu., A. Pahsa and A. A. Mert, "Intrusion detection sensors used by electronic security systems for critical facilities and infrastructures: a review", *Safety and Security Engineering VI 131*, 2015, pp. 131-141.

[11] A. Ross and V. L. Willson, "Independent Samples T-Test", *Basic and Advanced Statistical Tests*, 2017, pp. 13-16.