PROTOTYPE OF EARLY WARNING SYSTEM FOR HOME DOOR SECURITY BASED ON IOT USING PIEZOELECTRIC SENSOR

Abdul Hafizh, Nur Kholis, M Syariffuddien Zuhrie, Arif Widodo
Study Program Bachelor of Electrical Engineering, Faculty of Engineering, States University of Surabaya
abdulhafizh16050874053@mhs.unesa.ac.id
nurkholis@unesa.ac.id
zuhrie@unesa.ac.id
arifwidodo@unesa.ac.id

Abstract - Early warning system of door security based on IoT with a piezoelectric sensor, this was an early warning system that could detect a threat on the door and send a notification to the owner smartphone to do preventive action. This system was made at an affordable cost, which anyone can own this not only the rich one. This system will classify which a safe knock and a threat. This system used a piezoelectric sensor to monitor a threat and a buzzer to make some noise around. This system was equipped with a relay to control the solenoid lock as your primary lock. This system used Blynk cloud as the base which could be operated on the smartphone. The test used one room and one door. Take a survey to decide which a normal knock and a stroke. And as got the result, then set the setpoint based on the output voltage of the sensor, as a threat to the door. Wich that the microcontroller could send a notification to the Blynk apps on the smartphone. After that, we did some tests on the response time of, notification, buzzer, and the relay. Wich the response time of notification was 2,15 second, the buzzer was 1,1 second, and the relay was 1,15 second. This system has 80% accuracy. This system might be well monitored the door with Blynk apps.

Keyword: Security, Piezoelectric, Microcontroller, Notification, Buzzer, Blynk.

I. INTRODUCTION

Crime is an action that is detrimental to the victim and society, namely in the form of loss of balance, order, and peace.[1] moreover, it also applies to the extent of crime which targeting ownership rights that are already guaranteed by the constitution “every citizen have the right to own private property and it cannot be taken over arbitrarily by anyone “ [2] UUD1945 clause 28H verse 4. Thus, everyone is guaranteed ownership of personal assets or assets so that they are not taken by irresponsible people. According to the national statistical agency it has also experienced a decline in that 3 years.

Figure 1 shows the overall crime rate in Indonesia from 2017 to 2019 with a declining trend, where crime against other people's property has also decreased, as in the report of the state statistics agency.[3]. Figure 2 shows a very large crime rate still around, although it tends to decrease every year. Hence, we need prevention and early detection instruments of a crime that can be integrated by the internet using the IoT method "Internet of Things".

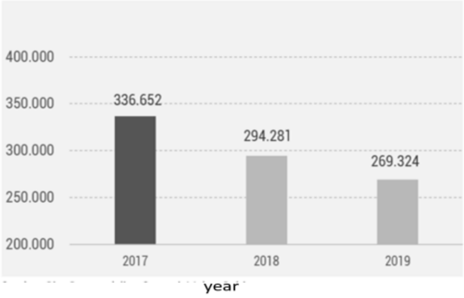


Figure. 1. Indonesia Criminal cases

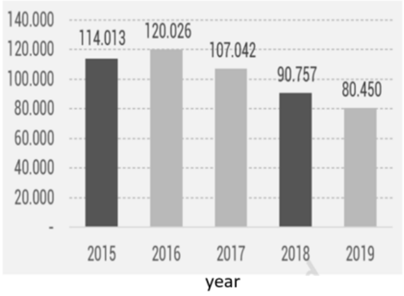


Fig. 2. Criminal cases on private assets
(Sources: badan pusat statistik nasional)

The development of technology in the electronics field has now reached the Internet of Things generation. Internet of Things (IoT) is a collection of things, in the form of physical devices (hardware / embedded systems) capable of exchanging information between information sources, service operators, or other devices connected to the system so that they can provide greater benefit in the infrastructure of the IoT that are embedded into the electronic hardware, software, sensors, and connectivity. [4][5]

The sensor used is a piezoelectric sensor, where this sensor uses the piezoelectric effect which can measure changes in pressure, acceleration, resistance or strength by converting it into an electric charge. This sensor is widely used to measure vibration, acceleration, and pressure. where this sensor will play a role in recognizing the type of knock and hit on the door while monitoring it. Furthermore, this sensor can be found in electronics stores at a low price. So that the entire community can enjoy the results of this experiment.[9]

The key is one of the home safety devices. A good home security system is greatly influenced by the quality of these keys. Various types of locks are used for home security systems ranging from manual locks to automatic locks that can be given a variety of security patterns. [5][6]

From the research that has been there, a lot has been discussed about door security systems. including research by Kaisar Malik Ibrahim and Iwan Krisnadi entitled "Design of Dual Security Home Door Systems Using Face and Fingerprint Recognition" which uses fingerprint sensors and webcams as a security verification process to grant access to open the door of the house for data processing. using raspberry pi 3. [7]

According to Alan Novi Tompunu, Yulian Mirza and Azwardi also discussed the door security system entitled "Room Door Security System Using Microcontroller-Based on E-KTP" which uses e-KTP as an access tool to the door and if 3 times missed the system will give a warning to the owner via SMS and for the microcontroller using Arduino.[8]

According to Adi Ahmad, and Muhammad Ikhlas also made an attractive door security system using a knock pattern, the research entitled "Door Opening System with a Pitched Knock Using ATMEGA 328 Microcontroller" where the piezoelectric sensor is used to read the knocks given and recorded by pressing the push-button when knocking on the door, the data obtained will be compared with previously stored data to be matched if it matches then the key will open.[9]

Based on the research that has been carried out above, the research that has been found only discusses the door security system by securing access to house keys but it can't monitor the condition of the door being safe or facing a threat. There is nothing wrong with the research above because even key security is a small part of the security system. and also some of the research above using research costs that are not cheap. Therefore this research is made to provide solutions for monitoring door security based on the conditions experienced by the door itself, not only how to access it, and also many other research publications about door security that are almost the same as the above, the only difference is the combination of access methods which will increase the cost required, and if the research is successful and being a mass product, only the middle and upper class who could enjoy the product. Where the lower middle class will not be able to afford it.

This research is also expected to be a solution so that the mid-low or lower class could use the products, and get a safer security system when traveling or working. Because all components of this study focus on functional components such as the use of node MCU instead of Arduino where node MCU is built-in with esp 8266 which can be connected directly to the wifi which Arduino with the same price or more expensive can't, and also the sensor used is a piezoelectric sensor which costs only 800 rupiahs for a single piece. This research may also be imperfect and can be developed or collaborated with previous researches.

The purpose of the study is to distinguish between threatening hits and ordinary knocks, to know the IoT-based door security early detection system work, and to analyze the accuracy of the IoT-based door security detection system. The benefits of this research are (1) providing an understanding of an internet-based system of things (2) providing a sense of security for homeowners when traveling because if there is something abnormal the system will send a danger notification.

The limitations of this research are, (1) using a Node MCU microcontroller (2) determining the type of beats based on a survey of beats from friends in the robotics design laboratory (3) the process of analyzing accuracy using an analog oscilloscope MOS - 9020 (4) using a door made from plywood instead of single wooden leaf. (5) notifications are sent via the Blynk application (6) using the Blynk application as the system interface.

The word piezoelectric is taken from Greek which has a meaning, namely, piezo is pressure and electric is electricity (electric current). Piezoelectric materials were first discovered by Jaques and Pierre in the 18th century. Where they work is to produce an electric field when the piezoelectric receives pressure. Piezoelectricity is a solid material that produces an electric field when exposed to tension, pressure, or mechanical vibration. Conversely, if the piezoelectric is charged, the material will experience tension, pressure, or mechanical vibrations. The piezoelectric sensor can be seen in Figure 3 below. [5][9]

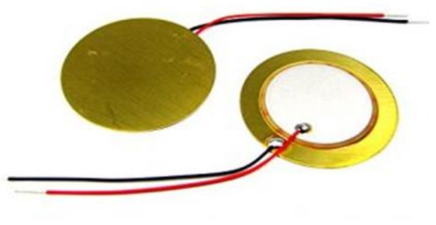


Fig. 3. Piezoelektrik Sensor
(source: http://www.insinyoer.com/prnisip_kerja_piezoelektrik)

II. METHODS

The research used a prototyping room with 1 main door to be tested. First, a literature study was carried out, then continued with making a system design, measuring the sensor value using an oscilloscope, and test the instrument when it was given a normal knock to a threatening hit, through a knock and hit type survey by taking samples from 10 different people. After obtaining the value of the required knock and hit types, the system's response time, and the accuracy test.

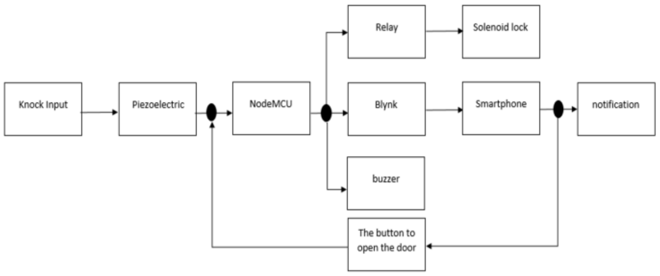


Figure 4. System diagram

Figure 4 above shows a block diagram of a prototype system for an IoT-based home door security system with a piezoelectric sensor. When the piezoelectric sensor detects a knock, the voltage generated by the sensor will be read by the node MCU, which becomes the microcontroller. When node MCU reads the sensor data and is found a threatening hit, node MCU will send a danger notification to Blynk, which will be forwarded to the owner's smartphone, in the form of a danger notification. At the same time node, MCU also gives the buzzer a command to sound, as a seeker for the attention of people around him.

In the smartphone section, besides providing danger warnings, smartphones can also be used as an access to open and lock the door. When it's given an order to open or lock the door via a button that has been made and aimed at the relay pin to run the solenoid lock, the command is sent to Blynk, Blynk will continue the command to node MCU. Node MCU who has received orders will order the relay to open or lock the door by charged the solenoid lock, through the relay switch according to the directions from the smartphone. where when the solenoid lock gets charged it will pull the door lock so that it can be opened, and when the voltage is cut off, the lock will return to its original position so that the door cannot be opened.

After the system design is made, a program will be made on the node MCU microcontroller to read the piezoelectric sensor value which will be converted into the sensor voltage value generated by the sensor with an analog oscilloscope as a reference for the voltage generated by the sensor. and this program must be able to provide a notification to the homeowner when something threatens the door and also pinned a buzzer on the door to provide noise which is expected to attract the attention of other people to monitor the source of the sound. can also access a home lock that can be opened and closed automatically using their smartphone.

The IoT-based home door security early warning system measures the reading of the sensor signal read by node MCU which is converted into a voltage using the analog oscilloscope MOS - 9020.By taking the peak value read on the oscilloscope compared to the highest value read on the microcontroller to be converted into a value the voltage generated by the sensor. The instrumentation process can be seen in Figure 5.

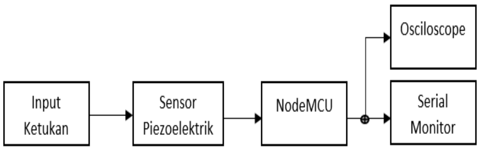


Fig. 5. Instrument measurement process diagram block

Where the door that has been planted the piezoelectric sensor is given a knock or tap randomly and the sensor readings read by Node MCU through the serial monitor will be compared with what is read by the oscilloscope. The oscilloscope is set with a peak value of 0.5V / div and a period of 0.5µs / div. In this process, the door will be removed from the room made to facilitate testing and also the position of the door to be more controlled, which can be seen in Figure 6.

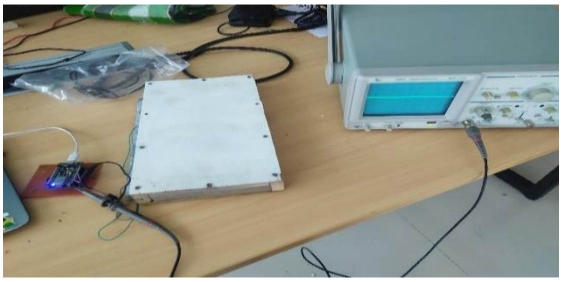


Fig. 6. Measurement process

III.
IV.

Furthermore, in the process of determining the knocks of ordinary people and a threaten hit, then the knock sampling is carried out in the robotics design laboratory by inviting students who are active in the lab to do the knocking they usually do where the voltage value was generated by the sensor will be read by node MCU and displayed. via the serial monitor. Then after getting the sensor voltage, the highest voltage value that is read on the serial monitor will be taken from each person who does the knock. Then proceed with the same thing as before, but the knock will be changed to a hard hit on the tested door to get the comparison results which will be used as a reference to define the input received by the sensor is still on the safe threshold or can be said to be threatening the door. Where the process can be seen in Figures 7 and 8.

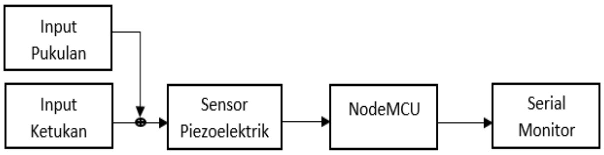


Fig. 7 Beating survey diagram block.

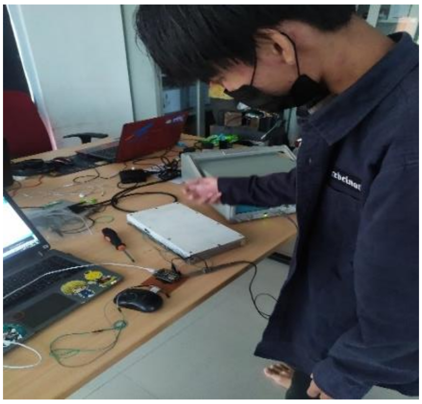


Fig. 8. Beating survey process

After the knock and the hit data is obtained, an Android-based application is made to provide a warning when someone tries to break it, or it can also be a key to enter the house.

After everything is ready, the response time is tested manually using a stopwatch from sending notifications, buzzers, and relays. To know the performance of the system respond to the time when it is used to give warnings and allowing access to the house, Its also performed accuracy testing using the analog oscilloscope MOS - 9020. With aims to verify the value of the sensor voltage read on the node MCU and oscilloscope, whether there is a miss or not.

III. RESULT AND DISCUSSION

First of all, make a container of the door security early warning system using a piezoelectric sensor for a door made of plywood and plant the piezoelectric sensor and the buzzer inside the door, and on the left there is space for a microcontroller and relay. The solenoid lock is placed on the right side. The front view of the room as shown in Figure 9.

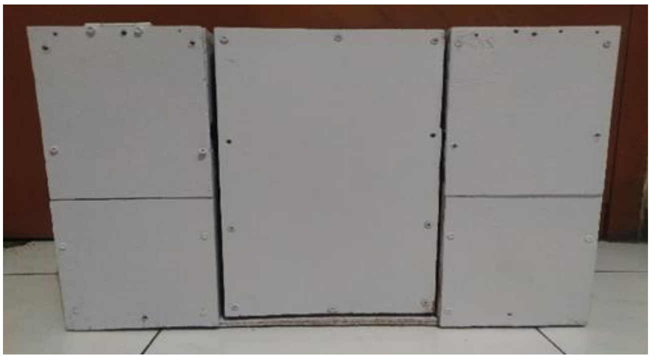


Fig. 9. Front room layout

Furthermore, the process of measuring the sensor value with an oscilloscope is carried out as a comparison of the value read by the microcontroller and by the oscilloscope in order to get the appropriate output value. By connecting the oscilloscope probe to the sensor output pin to be adjusted. The measurement results are presented in Table 1.

Table 1. is obtained from the oscilloscope setting set at a voltage of 0.5V / div and 0.5 µs / div which is matched with what the microcontroller reads by looking for the divider value to get the appropriate sensor output voltage. After the measurement is carried out, it is continued with the data collection process which will classify which knocks are said to be normal or facing a threatening situation. 10 people who are carrying out activities in the robotics design laboratory will be asked to knock on the door that has been given the sensor and has done previous calculations, to knock like knocking on doors in general. After getting knock data that can be said to be safe, they are asked to hit the door as hard as possible to get a break that can threaten the door.

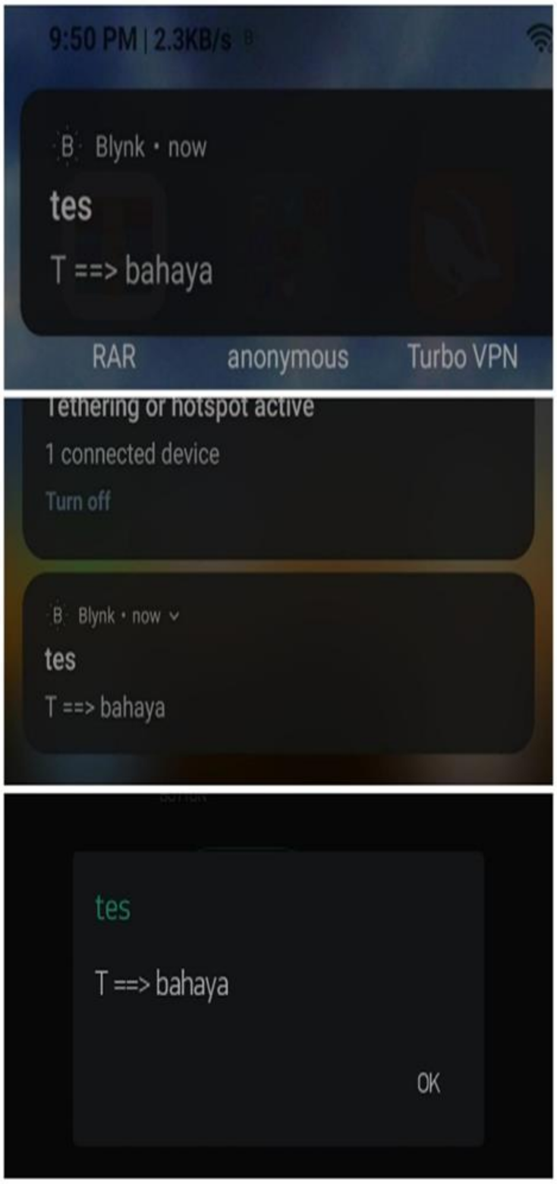
Table 1. Measurement system results

Measurement system results		
***Nodemcu* (bit)**	***Osciloscope* (Volt)**	***Nodemcu* (Volt)**
82	±0,4	0,4
40	±0,2	0,2
144	±0,7	0,69
173	±0,85	0,85
52	±0,25	0,24
163	±0,8	0,8
72	±0.35	0,36
93	±0.45	0,45
154	±0,75	0,75
163	±0,8	0,8

Table. 2. Knocking survey results

No.	**People sample-n**	**normal knocking (Volt)**	**Breakthrough attempt (Volt)**
1.	Sample -1	0,34	0,83
2.	Sample -2	0,3	0,76
3.	Sample -3	0,33	0,83
4.	Sample -4	0,2	0,65
5.	Sample -5	0,25	0,68
6.	Sample -6	0,37	0,74
7.	Sample -7	0,33	0,75
8.	Sample -8	0,24	0,72
9.	Sample -9	0,26	0,68
10.	Sample -10	0,4	0,85

Based on the data in the table below, the sensor voltage for the 4th person with the strongest knock has a voltage of 0.4V and the 10th person with the weakest impact with a voltage that reads 0.65V from the survey results. These results can be seen in Table 2. After obtaining the desired type of beat, the average voltage for normal knock is 0.3V and the average voltage for the hit is 0.75V. Next, do a programming process to determine the lower limit of unsafe bursts. where when there is a collision with the voltage above 0.65V, the buzzer will turn on and the microcontroller will notify the owner's smart phone. An overview of the notification received can be seen as in Figure 10



9:50 PM | 2.3KB/s

Blynk • now

tes

T ==> bahaya

RAR anonymous Turbo VPN

Tethering or hotspot active

1 connected device

Turn off

Blynk • now

tes

T ==> bahaya

tes

T ==> bahaya

OK

Fig. 10. Notification sent result sample

After obtaining the desired type of beat, the average voltage for normal knock is 0.3V and the average voltage for the hit is 0.75V. Next, do a programming process to determine the lower limit of unsafe bursts. where when there is a collision with the voltage above 0.65V, the buzzer will turn on and the microcontroller will notify the owner's smartphone. An overview of the notification received can be seen in Figure 10.

Furthermore, testing the respond time from sending notifications, buzzers, and relays. First, testing the response time of the notification sending which aims to find out how much time it takes to get the notification after the door has been hit hard. Then we get a graph as below. The results of measurement of notification respond time are shown in Figure 11.

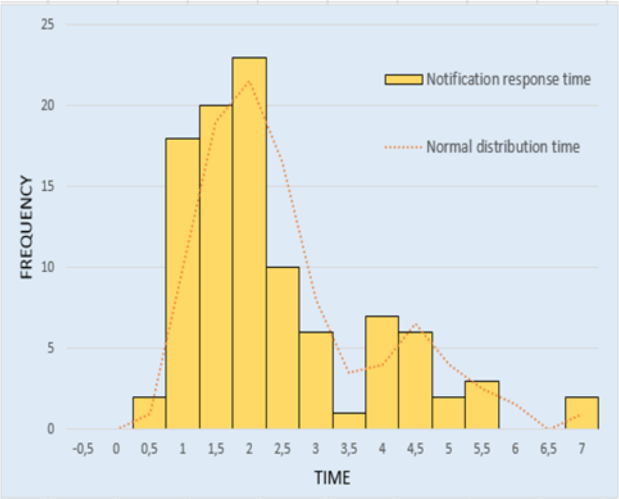


Fig. 11. Notification response time result Histogram.

From 100 experiments, the average notification response time obtained is 2.15 seconds.

After getting the results of the response time from the notification, it is followed by testing the response time of the buzzer as attention seeker where it works after the door has been broken, then the buzzer response time is obtained as shown in the graph as shown in Figure 12.

From the 100 experimental results, the average time result of the buzzer response is 1.1 seconds. After obtaining the results of the response time from the buzzer, it is followed by testing the time response of the relay as a switch to open and close the installed solenoid lock-based house key, by pressing the open button on the Blynk application. The results of this experiment can be seen in Figure 13.

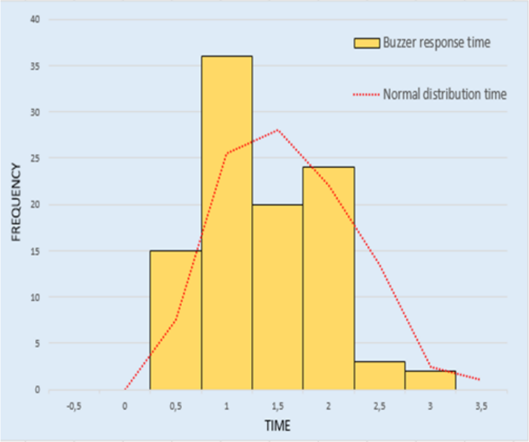


Fig. 12. Buzzerr respond time result histogram

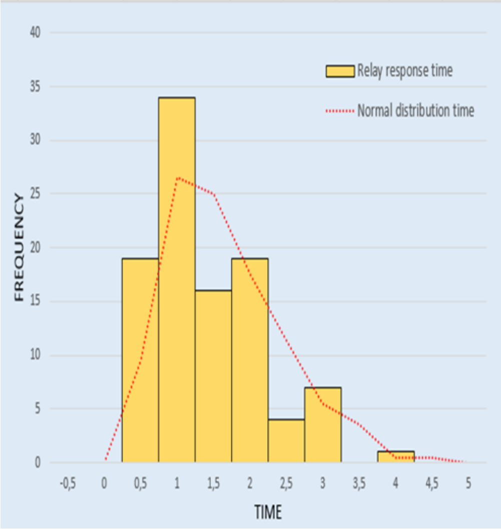


Fig. 13. Relay respond time result histogram

From 100 experiments, the average relay response time is 1.19 seconds.

Furthermore, the accuracy of the system is tested by comparing the output voltage value of the piezoelectric sensor read by the microcontroller with the one read by the oscilloscope. After combining all the existing programs several times the node MCU microcontroller reads the signal given to 0. Where it was done 100 times and 80 times correct or almost the same and 20 times detected very small. Due to the limited conversion capability of the ADC from the microcontroller. So from the data above, a confusion matrix table is obtained as shown in Table 3 below :

Tabel 3 The Matrix result calculation

MATRIx			
		Real Value	
		True	False
Predicted value	Positive	TP = 80	FP = 20
	Negative	TN = 0	FN = 0

$$Accuration\ Rate = \frac{TP+TN}{TP+TN+FP+FN} \times 100\% \text{ ....(1)}$$

The meaning of the abbreviation TP (true positive) is where you buy something that is positive and that is true, TN (true negative) is when you predict a negative result and the actual result is negative, FP (false positive) is when you predict the value that will come out positive but the results found are negative, FN (false negative) is a predictive value that is estimated to be negative but the results show a positive value.

Thus it can be seen that the accuracy value of the system being tested is 80%. These results occur due to the limited ability of node MCU to sample the input voltage signal provided by the piezoelectric sensor. Where the oscilloscope can read threats with reference voltages above 0.65V, while Node MCU reads very small sensor voltage signals, even 0V.

This result is influenced by the microcontroller sampling ability factor, tapping time, and the number of taps.

V. CONCLUSION

The conclusion of the research that has been made and tested is that the determination of the type of beat is carried out by a knock survey by 10 different people. Which is based on the sensor output pressure value that has been calibrated with an oscilloscope. This system works when it gets a sensor signal that indicates someone is trying to force the door to hit, where after getting the output voltage value above 0.65V, the microcontroller will send a notification of danger to the cellphone via the Blynk application, from the test results above, the accuracy value is obtained. this system is at 80%.

The advice that can be given is to try to use a microcontroller with better ADC conversion capabilities in order to get better accuracy.

REFERENCES

[1]. Soesilo, R. 1995. *Kitab Undang-Undang Hukum Pidana (kuhp) serta Komentar-Komentarnya Lengkap Pasal Demi Pasal.* Jakarta: Penerbit Politera.

[2]. MPR. 2002. *Undang Undang Dasar Negara Republik Indonesia Tahun 1945.* Jakarta : Majelis Permusyawaratan Rakyat. (https://dpr.go.id/jdih/uu1945 diakses pada: 30 Desember 2020)

[3].]BPS. 2020. *Statistik Kriminal 2020.* Jakarta: Penerbit Badan Statistik Nasional.

[4]. Sulistyanto, Muhammad , Nugraha Ahmad., 2015. *Implementasi IoT (Internet of Things) dalam pembelajaran di Universitas Kanjuruhan Malang*. Malag: (http://id.scribd.com/index. php/informatics/1 diakses pada: 30 Desember 2020)

[5]. Zanella, Andrea dan Vangelista Lorenzo. 2014. *Internet of Thing for Smart Cities.* Online: (http://ejournal.udayana.ac.id/index.php/informatics/1 diakses pada: 30 Desember 2020)

[6]. Helmi, Gunawan., Sumantri Yulianti., dan Haritman. 2013. *Rancang Bangun Magnetic Door Lock Menggunakan Keypad dan Selenoid Berbasis Mikrokontroler Arduino Uno.* Online: (http://jurnal.upi.edu/electrans diakes pada: 1 Oktober 2020*)*

[7]. Ibrahim, Kaisar Malik dan Iwan Krisnadi. 2020. *Rancang Bangun Dual Keamanan Sistem Pintu Rumah Menggunakan Pengenalan Wajah dan Sidik Jari.* Jakarta: Universitas Mercu Buana. (http://ejurnal.mercubuana.ac.id /index.php/jsakti/article/view/228 diakses pada: 7 Januari 2021)

[8] Alan, Novi Tompunu., Yulian Mirza., dan Azwardi. 2020. "*Room Door Security System Using Microcontroller-Based on E-KTP"* online: (https://ui.adsabs.harvard.edu/abs/2020JPhCS1500a2115 N /abstract diakses pada: 07 Januari 2021)

[9] Adi, Ahmad., dan Muhammad Ikhlas. 2020. *Sistem Membuka Pintu dengan Ketukan Bernada Menggunakan Mikrokontroller ATMEGA 328* Online: (http://ejurnal.tunasbangsa.ac.id **/index.php/jsakti/article/view/228 diakses pada: 7 Januari 2021)**