

Smart security door system using SMS based energy harvest

Abdullah Hamas¹, Amgad Muneer², Suliman Mohamed Fati³

^{1,2}School of Mechatronics Engineering, Asia Pacific University of Technology and Innovation, Malaysia

³College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia

Article Info

Article history:

Received Aug 13, 2020

Revised Oct 19, 2020

Accepted Dec 19, 2020

Keywords:

Energy harvest mechanism

GSM

Motion detection

Sliding lock door

Smart security door

ABSTRACT

Over the last decade, different studies have been conducted to increase security to identify sensor technology and provide alternative energy with other energy harvest techniques such as vibration energy harvester and sun energy harvester. There is no combinational approach to utilize the door to create energy and use it for security measures in the literature, making our system different and unique. This proposed system comprises the security and the energy harvest; the security section utilizes a motion detector sensor to detect intruders. For instance, the magnetic door lock type firmly locks the door, which can only open with a generated password. On the other side, the energy harvest section utilizes the door motion to generate electricity for the system, which solves power shortage and limited battery life issues. Moreover, this study includes a GSM module that allows authorized owners to receive a generated password as a security enhancement. This design mainly focuses on improving or optimizing the conventional security doors' overall performance as sliding door, panel door, or revolving door. The experimental results show the system efficiency in terms of power generation and the time needed to authenticate the property owner. Notably, the power generator can generate electricity more rapidly, while the needed time to receive the mobile device's security code is around 3.6 seconds.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Amgad Muneer

School of Mechatronics Engineering

Asia Pacific University

Technology Park, 57000 Bukit Jalil, Kuala Lumpur, Malaysia

Email: muneeramgad@gmail.com

1. INTRODUCTION

Many people are aware of the danger of using the traditional door padlocks for home protection due to the ease of breaking these padlocks. For instance, unauthorized people like thieves or fraud can forge keys or make a new master key to access the house without being detected. Therefore, to eliminate the problem of insecurity issues utilized in the traditional method, the usage of motion detection sensors, GSM, and auto-generated password door technology is highly recommended [1-3], whereby the motion detectors are used to detect the intruders. In contrast, a password can be used as an authentication mechanism. Several enhancements have been implemented to improve the door security, such as password complexity in terms of length and special characters and a one-time password sent to the registered mobile number. This one-time password should be changed every time, aiming to reduce the human burden to memorize the password and avoid password theft [4]. In recent years, many researchers have work on making the entrance door more intelligent and secured with the help of human identification sensors technology [5-8] like fingerprint reader [9], voice recognition [10], RFID [11], and others [12, 13].

Worth mentioning, these security approaches lack sustainability and reliability, where they rely on the limited power supply as batteries. Therefore, one possible enhancement for these systems is utilizing the door motions to provide an alternative electrical energy source. Hence, additional research has been conducted on generating renewable energy [14-19]. According to the literature review, the energy harvest technique is the latest trend to sustain energy [20]. In addition to the efficiency enhancement, these energy harvest techniques also provide a means to supply power for the micro wireless device and other devices where low power consumption is needed.

Harvest concept is to scavenge the energy that can be found or available in the surroundings to convert it into usable electrical power [21], which has less popularity and needs to investigate its applicability in the real-life fields, including door security. Energy can be harvest from a different source such as thermal, vibration, motion, or mechanical source [22] with various mechanisms such as relative motion, vibration [23], heat, and others. However, it was recorded that energy harvest from vibration or thermal has less impact on overall power generation but improves daily. Therefore, utilizing sliding doors for energy harvest is promising, particularly in places with crowds and frequent door motions like hotels, malls, schools, universities, and airports. The frequent movement of the door is a good source of energy that is wasted. This idea is a good practice for green renewable energy [24] to reduce traditional power generators' emissions. In this proposed work, the type of energy harvester proposed in this work is a rotational energy harvest technique using a sliding door and DC generator. This type of energy harvest requires a continuous rotation to attain maximum efficiency. However, continuous motion is difficult to attain. Therefore, power storage, *e.g.*, a battery, should be used to ensure energy continuity during the closing hours or idle hours.

Therefore, this paper's contribution is threefold: developing a smart security system with self-generation energy using energy harvest technique with power-saving for future use. Second, implement a GSM-based authentication and alert module, authenticating the owners through one-time passwords and sending a warning for any suspected intruders. Third, develop an antitheft mode system using a motion detector sensor with a keypad security lock system, including magnetic lock devices, as security enhancements for the proposed approach. All these modules are integrated and experimented with observing the response times and the reliability of the system.

The rest of the paper is structured as follows: Section 2 describes and summarizes a few research pieces related to the proposed study. Section 3 gives an overview of the methodology adopted for the proposed research and a description of the software implementation. Results are discussed in section 4, while; the conclusion and the future work are given in section 5.

2. RELATED WORK

Intensive research works were conducted on the door lock security system. Door lock security systems can classify into different categories according to the technology used. These systems are password-based, GSM-based system, biometric-based system, RFID-based system, smartcard-based, motion detector-based, VB-based, and hybrid systems, which combine two or more of the aforementioned examples. In the following lines, we are going to discuss these examples.

2.1. GSM based systems

In most door lock systems, the most common means of communication is done via GSM technology. The majority of design adopts a concept of actuation GSM communication via a controller to send messages in an emergency to the respective owner or user related to security at the break-in time. For a GSM-based system to work as an obstacle or theft detector, the system requires different sensors. This sensor helps such an approach to gather the information that needs to send based on instruction or commands [25]. The current usage of the GSM-based system utilizes it as a remote control transmitter and receiver with a motor door to automatically control the motor via control from a based station or remotely.

2.2. Biometric-based system

This biometric-based system is one of the standard methods adopted in a situation where the user's behavioral or physical part is required for door authorization. A typical example is a fingerprint-based system that requires a user's palm or finger to lock and unlocks the door; this helps verify the right owner and reduce the chance or error [26]. Biometric techniques become very useful in bank lockers as they provide a more accurate result with high-security efficiency. The common mode of configuration is utilizing a microcontroller with biometric devices for a continuous monitor of the intruder through a keypad, camera, iris scanner, or vein detector [27]. Some configuration utilizes wireless motion detector sensor at night to sense intruder and trigger alert through microcontroller.

2.3. Motion sensor and detector-based systems

The motion detector utilizes a motion sensor whose working principle is based on the amount of light on the photodiode component. The photodiode sensor usually reads a maximum of 255 decimal if the light keeps falling on the photodiode surface. However, if the light is hindered or becomes less, the voltage produce will be less than 50 in decimals [28]. In this situation, the system triggers an alarm or serves as an alert signal to another device actuator.

2.4. Door phone-based

Phone-based is a type of door security that identification is made via direct communication from visitors to the housing owner via the security control section department. This scheme usually comprises of hand-free phones by housing owners. Some are configured to allow the user to pass through the gate with some voice instructions through the phone to the system. This system has an upgrade to the door phone surveillance system that technically utilizes to identify visitors [29]. De Lima *et al.* [12] have introduced a smart door lock system based on a mobile app and Bluetooth technology. It provides features of auto-lock, schedule lock, and security door lock.

2.5. Combine system

This type of lock security system utilizes multiple security control techniques via a controller. It could comprise password-based type, fingerprint, RFID, GSM technology to initiate the authentication [30] or authorize performance. This scheme helps to lock and unlock the door in real-time. Tshomo *et al.* [11] proposed a dual locking method using RFID and fingerprint recognition. It is a safe and effective locking device installed in the home, workplaces, schools, and any organization. Even if the users lose the RFID key, their fingerprints will unlatch the lock. Only approved users can use their fingerprints and RFID tags to access these. If any unauthorized persons attempt to access it, first of all, the short message service (SMS) will send a text message to an owner using a global mobile communications system (GSM) [31-33].

2.6. Energy harvest system

The energy harvest system is a type of system that utilizes to extract energy from the environment and convert them into usable electricity, while other research has been conducted on energy harvest. The generation of energy from moving structures has been more research area, most recently in place of wireless sensor powering. In contrast, most energy harvest system is initial, drawing power from the frame's relative motion that suspends an oscillating proof mass [14]. This initial proof mass produces counter force to produce by motion source in which no second point of attachment is in need. This scheme provides a means of possible application and installation, while other report devices utilize linear motion between mass and frame. However, another possibility of rotating motion, indeed, rotating initial mass generator found more suitable and become more commercially successful.

A typical example is their wristwatch utilization, whereby utilizing proof mass and center offset the rotation axis, the rotation device can drive by rotational or linear source motion [15]. Due to counter force that may result from frame acceleration, energy may not harvest or generated efficiently as a constant rotation of host motion in both rotational type and linear type. For body motion power devices such as device power from a revolving door generator or wristwatch generator, constant rotation is not available. While revolving door usually undergoes a continuous rotation in many cases [16]. This review focuses more on energy harvest from rotational motion or door. Therefore, research is conducted to harvest energy from a revolving door through a rotational movement and convert it into electricity. The entry design is a four-panel type revolving door that allows users to rotate at 180 degrees rather than three-panels that only allow 120 degrees rotation-theoretical design of the door done with AutoCAD. Different material was selected for an entry during fabrication, such as the revolving door section to be Perspex with 3 mm of thickness. Another essential material selection is the generator and gear. Therefore, 120 RPM with 1500 mA, which can produce 5 V to 24 V generator, was selected. The testing procedure carries out average current through time from three different plotted simulations, and the power output was calculated and recorded. The final result indicated that 15.67 Joules of electricity could generate by one push door with a selected generator [16].

The system door is designed to generate electricity and to monitor the activity of the user approach. This system is classified under low-power instrumentation. The design comprises a coil and magnet at the door's roller side, including a battery that is all installed carefully without damaging the door. In this approach, the energy source being studied here is humans that open or close a public building door. The system focuses on the public because the door will open and close several times; in this case, more energy can generate from the door rotation through the calibrated coil and magnet. Therefore, the complete prototype utilizes smart power management, low-power electronic devices, and portable battery to measure door usage characteristics [34] efficiently.

Door based generator approach which automatic open and close, the primary target of this project is to provide the solution to the shortage of electricity with the help of the existing home door. In this project, the revolution door is studied while it sources rotational mechanical energy is converted into an electrical entry with DC generator and store for further usage. The project construction comprises several components, including a pulley that attaches to the stepper motor utilizing a belt to transfer the rotational motor to generate electricity. Different testing was done while the final voltage and currently achieved at approximately 12 V with 0.1 Amps [19]. The design of an energy harvest-based door, which approaches linear motion, was also studied. This design has 1g proof mass with an oscillation amplitude of 5 mm as it could produce up to 200 uW. The work also estimated that further work could produce more power in the future depends on the type of motor and motor speed [35]. To provide the necessary amount of clean energy approach, the authors fabricated a revolving door, amplifying the door shaft initial RPM and motor mechanism utilized to generate energy. The system comprises a bridge circuit that smooth the electrical generated DC voltage generated by the motor for power utilization and storage purpose while the door extracts energy through a motor arrangement, gear, and pinion. Alternatively, energy is produced by harnessing the power that a human dissipates through the door. Therefore, as the door opens, this will revolve the integrated gear connected to the door, linking gear to the DC motor will cause the motor to produce electricity while the bridge circuit filters voltage generated and output voltage utilize to charge a battery [36].

2.7. Related work on the security lock

In [37], a wireless security system was proposed whereby the system's alarm program was implemented on GUI, and the system design to monitor the RFID tag and reader also includes monitoring the GSM terminal. The method implies in this system allows tag information to be sent to the server. Therefore, when the laptop is stolen from the region that the RF is covered, the alarm will trigger while the security measurement allows the stolen item owner to be alert through SMS. The system is useful for property protection at home and offices.

Another functional approach for door security and locking system is based on GSM technology and password done by [38]. The procedure is to control the door security measurement using GSM technology remotely. In this development, one GSM module act as a receiver with a DTMF decoder connected to the microcontroller, which is attached to the motor at the door side while the other GSM act as a transmitter, in this case, it can be a mobile phone, the design adopted can categorize into controlling decoding, GSM and switching. However, GSM utilizes as transmitter and receiver that set instruction of control command through mobile phone to door, while DTMF decodes this signal to perform users' instruction, control, and the motor is then initialized via microcontroller while door will open or close via switching techniques [38]. Similar work is done by [39]. The system allows the door to control remotely using a GSM network. The system comprises a relay switch that enables the door to close or open, a buzzer for alarm in a situation whereby the right command is not received by GSM module to 8051 microcontrollers as a control unit and power supply 5 V DC to microcontroller unit, GSM module, and relay module. The system allows users to enter access code through the phone, therefore if the code is correct, the user will enter the room, but if it is wrong three times, the alarm will trigger which denote emergency condition. The final prototype thrived, and the result was obtaining.

Eseosa and Promise conducted a similar approach in [40] whereby a smart and intelligent security system for the intrusion detection approach finds a solution to conventional security system limitations in real-time monitoring and control of household or door activities. The overall system design comprises GSM technology for sending an intruder's real-time messages to the owner, PIR sensor as intrusion sensor, smoke or fire detector sensor, gas sensor, buzzer, and relay switch, and all are embedding to a single controller unit. Code implemented in C language and design and analysis model and simulated with Proteus, final prototype develops based on the design circuit diagram. Moreover, Oke *et al.* proposed another door security model in [41] whereby a smart card and Bluetooth have been used. The smart card framework design only allows authorized to perform to get a safe entry with only a smart RFID card before passing through the door while all activities control with microcontroller output. However, Bluetooth is used as a communication medium, usually simple and very productive, though more suitable for shorter range security control and monitoring system; this system utilizes an Arduino microcontroller while solenoid act as output [42].

As a conclusion for this section, intensive research was conducted and, there is no combinational approach to utilizing the door to create energy and to use it as a security measure, which makes our proposed system novel and unique. Our proposed system fills the security and renewable energy gap by integrating the two concepts, security, and energy harvest system. The security section utilizes a motion detector sensor to detect intruders. However, the magnetic door lock type uses to firmly lock the door, which can only open with a generated password. This study also includes GSM technology that facilitates authentication through a one-time password being sent to the owner's device. Therefore, this design mainly focuses on improving or

optimizing the overall performance of the conventional door. Thus, the sliding door was implemented in this study because it harvests more energy compared to a panel door or revolving door.

3. RESEARCH METHOD

In this study, the proposed methodology is divided into two stages: the security and energy harvest sides. Figure 1 describes the security side of the programming language. This scheme comprises the code of intruder detection sensor, password generation, keypad, a display unit (LCD), LED indicators, an alarm system, and SMS sender module. The proposed system starts with variable initialization. The sequence of the code begins by generating a 5-digit password upon the user's detection. The program then allows the password generated to be sent to the registered phone number (owner) through SMS. However, whenever a human is detected, and the user tends to type in his or her password, the programming code tends to wait for a few minutes to determine if the user is an intruder. Once the user enters the wrong password three times, the detected person will be considered an intruder. An alarm will trigger, which also includes an intruder message on the LCD screen. However, in a situation whereby the password typed is correct, the door will automatically unlock as an authorized user, and LCD will display a message that indicated that the user is allowed to enter.

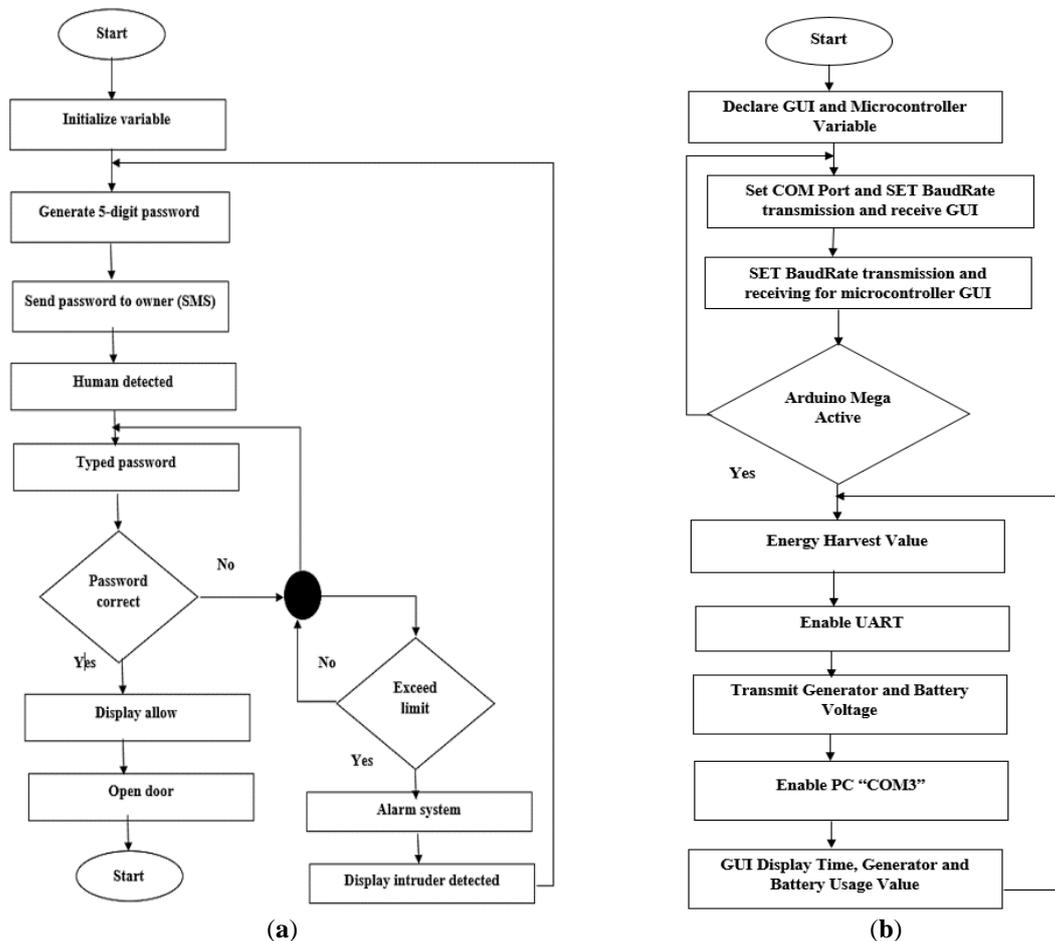


Figure 1. Flow cart of (a) Security side of the proposed smart door system; and (b) Signal flow for the proposed system

Figure 1(b) described the energy harvest side of the system. This side of the code is programmed to read analog data from the DC generator and battery, which are to send to the computer (MATLAB) for display and analysis purposes. The program begins with a declaration of all necessary parameters on MATLAB and Arduino MEGA microcontroller while port and baud rate were set to match. In this case,

9600 bps baud rate was selected to match UART communication speed between the microcontroller and MATLAB. Moreover, once generator voltage and battery were measured, both will send sequentially to MATLAB through enabling UART communication, successively in this meaning termed as serial communication. This setup utilizes COM port 3. This can vary from one system to another. In this work, COM 3 was selected as the available communication channel for data sharing data between the computer and Arduino MEGA microcontroller. Therefore, as soon as this data transmit to MATLAB (computer), MATLAB code will process and split out both energy harvest voltage from the generator and the amount of voltage stored in the battery. These are displayed through a text box design with GUI. However, GUI will always show full battery status as soon as the battery voltage is greater than 3 volts as programmed.

Furthermore, this study was implemented utilizing several major hardware modules range from Arduino MEGA microcontroller, PIR motion detector sensor, 16x2 LCD, circuited 12 VDC and 5 VDC power supply, 5 VDC relay, magnetic lock, buzzer (sound system), GSM modem, DC generator, LED's indicators and 4x4 keypad. All this major electrical component was circuited together as per the given circuit diagram to develop the smart security energy harvest door system.

3.1. Power supply

The power supply is significant in this study as it utilizes a DC adapter that converts 240 VAC to 12 VDC. However, the circuited power supply comprises an LM7805 voltage regulator chip. In contrast, the 10 uf capacitor and 1uf capacitor connected in parallel at each side of the voltage regulator chip, the voltage regulator chip allows the 12 VDC to regulate into 5 VDC and switch connected in series to the supplied 12 VDC, this is to turn OFF and ON the system at any time wanted, 10 uf and 1 uf capacitor help to ripple unwanted AC signal from the circuit. However, the primary purpose of utilizing two different power sources, such as 12 VDC and 5 VDC, which is the selected magnetic lock can energize by 12 VDC, though some can energize by 5 VDC. Moreover, 5 VDC has utilized to supply power to all modules such as the GSM module, PIR motion detector sensor, and relay circuit and can also use to power the ARDUINO MEGA microcontroller if deciding not to power it with a computer via USB (*i.e.*, if the system is dependent from computer connection). The 330 resistor circuit in series with LED-RED indicates if power is ON or in OFF state when providing 5 VDC to all modules, as depicted in Figure 2(a).

3.2. Door lock circuit

Figure 2(c) shows the circuit diagram, which comprises of the relay connected as a switch to 2n222 NPN BJT transistor circuit, that is, the relay will only energize when voltage is applied to the base of the transistor, transistor collector connected to 5 VDC is the circuited power supply. In contrast, the ground is connected to PIN 4 of the microcontroller, two different switches connected to the relay to energize and de-energize the magnetic lock when required. The primary purpose is to keep the system flexible, therefore if the magnetic lock type is to energize with 12 VDC or 5 VDC, users can switch ON 12 VDC switch or 5 VDC switch respectively, so it will eliminate new circuit board design in a situation when magnetic lock type is change. In this circuit connection, whenever an intruder is detected, PIN 4 of the Arduino MEGA microcontroller is HIGH. This will trigger the relay to allow 12 VDC or 5 VDC to pass through to reach the magnetic door lock and energize it. In another way, once the microcontroller sends a low signal, relay switch, and no connection between the magnetic door lock and power source, then the magnetic door lock will energize. Energize and de-energize magnetic door lock use in this study means locking the door or opening the door.

3.3. Indicators and alarm system

This is a vital circuit, as it is beneficial for users' interaction. Two different LEDs and one speaker (buzzer) were utilized to interact with the user. One LED is to indicate when the door is fully locked or open, and the other LED is to show the user is authenticated by sending the password to his/her device once the light blinks (ON for a while). As depicted in Figure 3(a), LED door lock (D1) and LED password indicator (D3) connected through a 330 ohms resistor to PIN 5 and PIN 7 of the Arduino MEGA microcontroller, respectively. In contrast, the speaker which has two PIN out such as the positive that connected to PIN 2 of microcontroller and the negative connected to ground, this speaker will beep when the password is wrong and willfully trigger the alarm when password entered exceed it trier limit.

3.4. Keypad and other pinout labels

The keypad comprises row and column pin out circuited directly to the Arduino MEGA microcontroller. The row pin is 8, 7, 6, 5, while the column pin is 4, 3, 2, 1. This is circuited to microcontroller pin 15, 14, 13, 12, and 11, 10, 9, 8, respectively; a typical way to understand how the circuit work is to examine one keypress input. For example, whenever row 8 and column 4 are low, it means when

press, this will indicate that keypad “1” is press; also, when row 8 and column 3 are short, this will indicate that keypad “2” is a press. This process is the same for all other keypad press. Typically, the project only utilizes keypad 0-9, while the alphabet and alphanumeric keys can be ignoring. Figure 2(d) shows the details of the Keypad circuit.

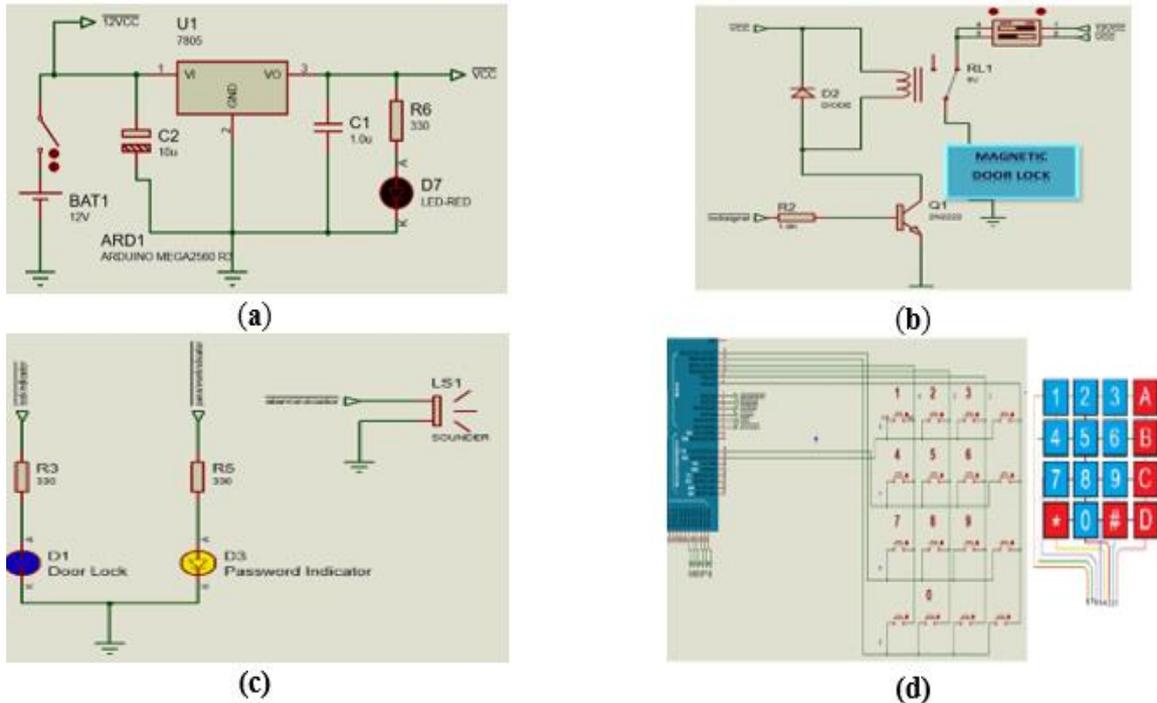


Figure 2. Schematic diagram of (a) Power supply circuit; (b) Magnetic door lock circuit diagram, (c) Alarm and LED indicators circuit and; (d) Keypad circuit diagram

3.5. SMS unit

This unit, as shown in Figure 3(a), comprises of GSM module along with valid SIM Card, module consist of 4 major pin out which they are VCC, ground, TX and RX, VCC is to connect to 5 VDC of power supply and ground is connect to common ground of the circuit, major aspect is the TX and RX pin which connected to PIN 19 (RX1) and PIN 18 (TX1) of Arduino MEGA microcontroller. This connection allow microcontroller to communicate with GSM module using AT command. It is the main method for sending generated password through SMS to house or room owner.

3.6. Motion sensor and reset password button

This circuit section, as shown in Figure 3(b), consists of motion detector circuit and manual password reset circuit, motion detector typically have three main PIN out, this are VCC, OUT and GND, this are connecting to 5 VDC, PIN 3 of microcontroller and common ground respectively. However OUT PIN connected to microcontroller PIN 3 is the PIN that provide when motion detect as HIGH and when no motion is detect as LOW. Reset generated password button connected to VCC with 10 Kohms pull up resistor while the output connected to PIN 6 of microcontroller, in this circuit, PIN 6 will always HIGH but will LOW as soon as the push button is press.

3.7. Generator and storage unit

DC Generator in this study is a rolling mechanism that helps to convert of rotational motion into electrical energy; this is easily done by the DC generator anytime it rotates, the principle behind this can well explain from Michael faradays electromagnetic principle which lets to understand the basic concept behind the production of electricity from magnetic field. The generated voltage read through PIN A0 of Arduino MEGA which battery voltage read though analogue PIN A1 of Arduino MEGA, the circuit also comprise of load LED, this is to test and visualize the voltage generated, multiple LED's or bulb can utilize load testing. The circuited diode prevents the motor from automatic rotation when connecting to the battery, so it remains

as DC generator rather than working as a motor, as depicted in Figure 3(c). Using SolidWorks software, the smart security door harvesting energy has been designed as illustrates in Figure 4. The security part contains the LCD and the keypad for enter the password further Arduino and SMS module. The motion sensor is placed on top of the sliding door, as illustrates in Figure 4. Eventually, the energy harvest part contains DC motor and battery, as illustrated in Figure 3(d).

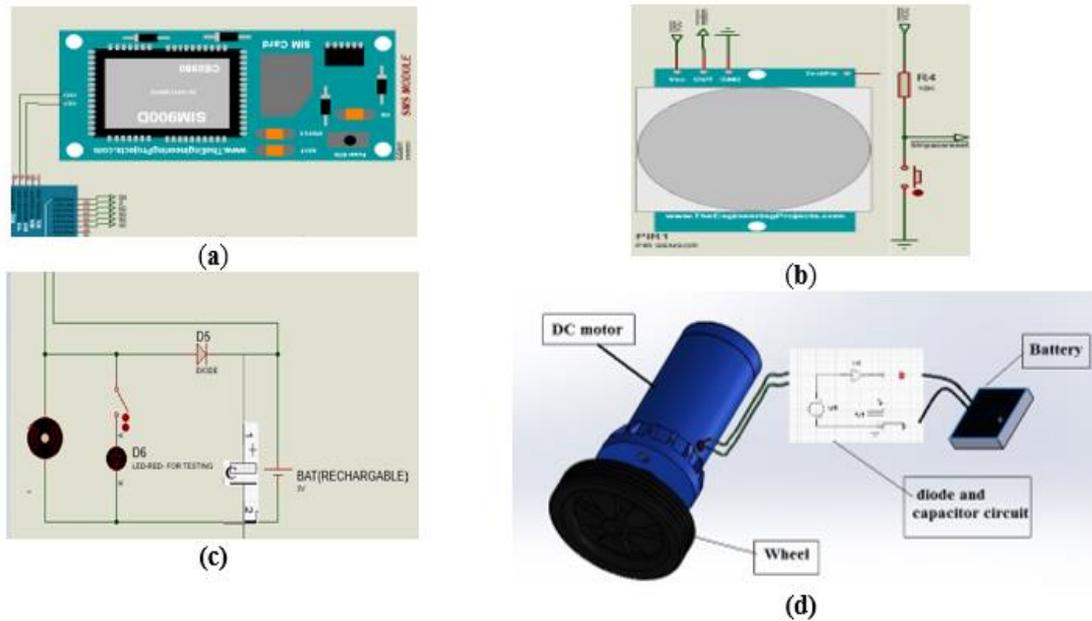


Figure 3. Schematic diagram of, (a) GSM module wiring; (b) Motion sensor and reset button wiring, (c) DC generator for energy harvest and storage unit circuit; and (d) The proposed security and energy harvest system container

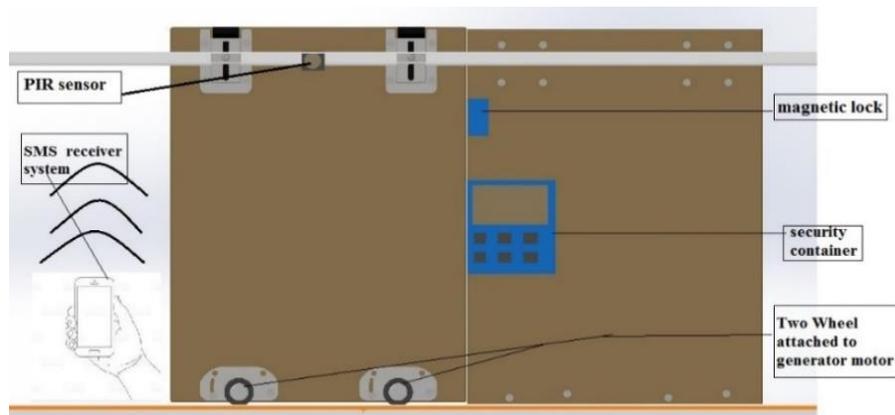


Figure 4. The scenario of the proposed experimental system

4. RESULTS AND DISCUSSION

Smart security door energy harvest system is a multi-purpose system design to improve entrance door security yet scavenge electricity from the door. Therefore, it comprises two major sections, which are the security side and the energy harvest side. According to the developed security side, the door is designed to sense the presence of human activity at its entrance with SMS sending capability, automatic door lock, indicator, and alarm system, and keypad button. The working process included that the system will generate a security password and send it to authorize owner, in the situation when someone approaches the door, the motion detection sensor will quickly detect the person within seconds. However, if it is authorized or rightful

owner, the system believes that, authorize owner would have a valid security password to enter the room without notice as an intruder, in this situation, the motion detection sensor keep scanning for movement and send it to the controller of the system, if the person that approaches the door is taking a longer time than usual, the system will believe the person is intruder and alarm will be trigger include intruder warning display.

Another intruder detection that designs along with the system is when the user tries more than the required password (exceed 5); however, as the user types the wrong password, the sound will beep, but when exceedingly more than 5 tries, intruder alarm will trigger, and a new password will also have regenerated and sent to registered owner (authorized person) phone. A few indicators and a reset button design along with the system, LED blue indicators will allow the owner to know that the magnetic door is locked when the LED is ON while the second LED indicator, yellow, will blink once the new password is generated. The reset button allows the owner to manually reset or generate a new password at any time, this is to allow the owner to also have a password reset control over the system should incase the owner lose the generated password send to the owner through SMS message via accidentally message delete and others. Moreover, sliding door constructed with a homemade material range from wood, nails, hardboard, roller, and two DC generators. The construction method is a form of cascading whereby all pillars are constructed one after the other as per design, the sliding door section attached to roller while this roller attached as a link to DC generator with multiple gears as given in Figure 5(a). According to Figure 5(b), the roller (tire) would allow the DC generator to generate electricity as it rotates these two generators upon sliding back and forth. The slider door channel hangs the sliding door to the housing while all support cascades to provide better housing for the proposed system.

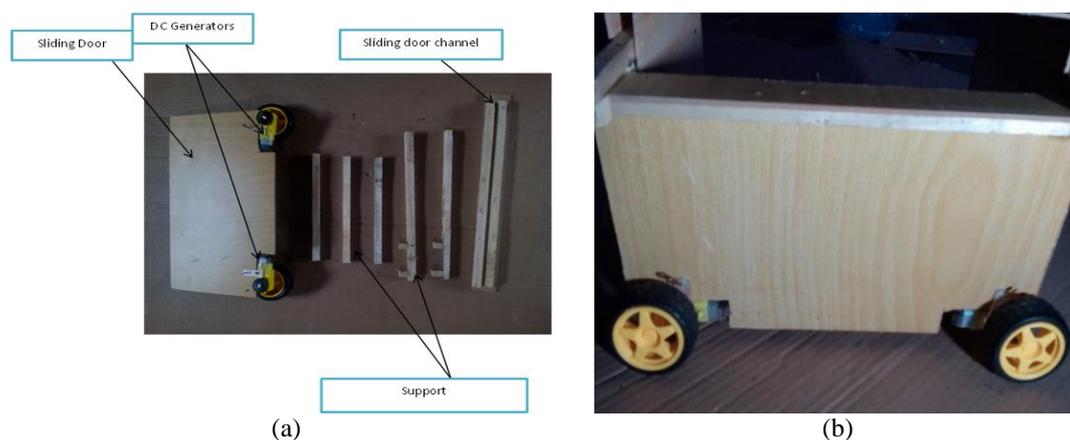


Figure 5. Construction method; (a) Sliding door parts, (b) Sliding door Front view with two DC generator for harvesting energy

Regarding the developed energy harvest section, the final experimental model utilizes two micro-DC generator, the primary reason is to ensure that energy is harvest from the back and forth of the sliding door, the energy that is harvest from the DC generators then store in a two-finger rechargeable battery, this is 1.5 volts each connected in series to provide 3 volts' battery capability. However, both DC generator and battery voltage monitor with MATLAB GUI. It comprises of start and stops button, which tells the program when to start accepting data from the microcontroller, text boxes design to insert DC generator value and battery voltage; a status bar also designs to alert the energy harvest supervisor when the battery is full. Figure 6(a) shows the experimental model of the proposed system, and Figure 6(b) illustrates the results of the motion detection.

The security system begins with a welcome message; however, the password was generated, which is sent to the user phone, as shown in Figure 7 (a-c). During this period, two LEDs help to understand that door is lock and a password has been generated as shown in Figure 7(d). Further instruction displays on LCD as shown in Figure 7(a). The sequence result provided that if the password is correct, the magnetic door light is off, magnetic door de-energizes, door open, LED blue is OFF, and entering allowed is displayed in Figure 7(e). However, when it is the wrong password as presented in Figure 7(f), this means that the door remain lock and sound help users understand that wrong password is being pressed; however, if wrong press more than 5 times, alarm trigger while reset button can use to reset new password and stop the alarm.

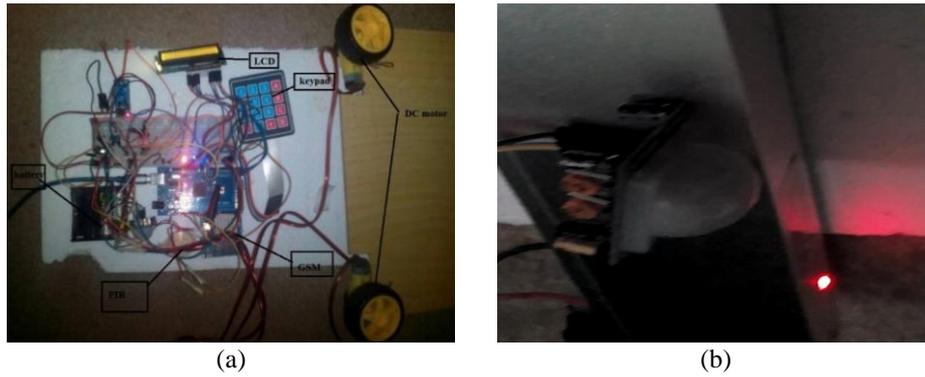


Figure 6. Experimental model of (a) smart security door energy harvest system and (b) Motion detected door remains lock as the LED is ON, will only be off when correct password enters

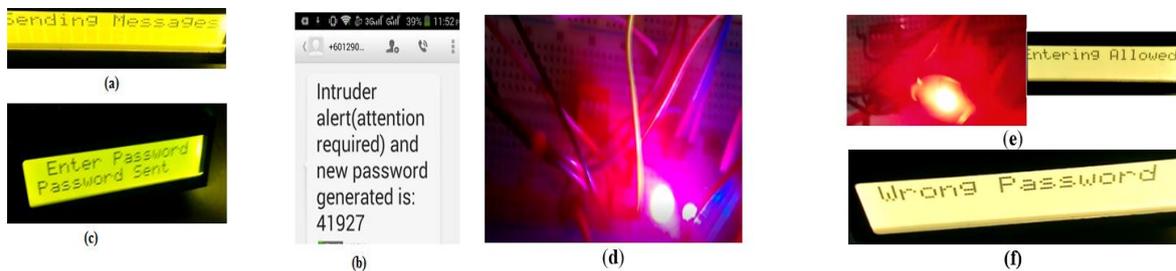


Figure 7. Experimental result of; (a) Password generated is sending to phone; (b) Generated password received by an authorized person; (c) This is status when the password has been sent, (d) LEDs while the blue light ON indicated that door is lock and the red light on indicated that password generated has been sent; (e) Password correct, LED blue is off and entering is allowed; (f) When user type wrong password, while 5 times trying entering a wrong password will trigger the alarm

Figure 8 shows the designed energy harvest GUI to show the voltage generated in real-time from DC generator and rechargeable battery. This GUI also has a start button that allows users to start ready data from sliding door through microcontroller and serial communication while stop will instruct the program to stop reading or measuring energy harvest system. The GUI also includes the time that can help the operator record a specific time based on the amount of voltage energy stored in the battery. Figure 8 depicts energy harvest results.

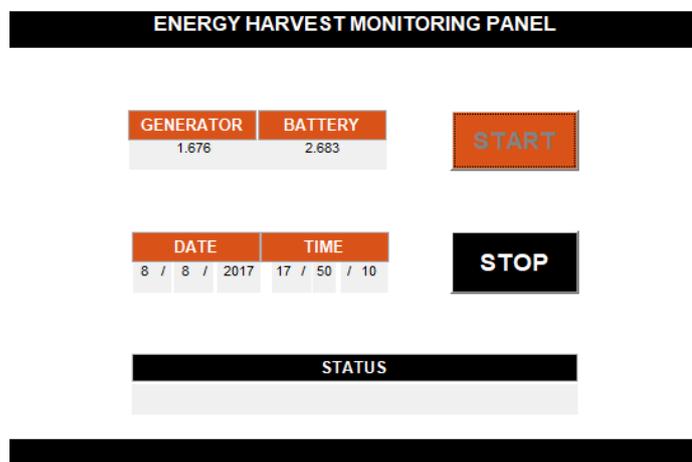


Figure 8. A voltage of DC generator and battery monitoring as start button was press

4.1. Motion sensor

The test motion sensor was first recognized, and data was collected based on the output of the system. Data was collected in a sequence of the time intervals where motion ranges in terms of the output voltage which being analyzed. As shown in Figure 9(a), the voltage and frequency (see voltage read) change with respect to the distance. This means the sensor's output is highly sensitive with respect to the distance (the range). In addition, the analog values indicate the changes in detection with respect to the motion. This means, the nearer the motion from the sensor, the higher voltage changes into the analog read value. The advantage from analog reading is to get the sharp range for the sensor changes in the output. When it comes to the Arduino part, this analog read value ranges from 0 to 1023 MV, whereas the sensor value range begins the changes into voltage from 0 to 900 MV. Figure 9(a) shows the motion sensor range vs. voltage.

4.2. SMS average time text received

This experiment is carried out to understand the delivery time of sent SMS by the system because password generated to enter the house or unlock the security door is only sent to authorize owner through text message (Phone). Therefore, it becomes necessary for the owner to understand his waiting time whenever the new password is generated. However, the usual delivery time of SMS message by the end-user should be between 1-3 seconds, while this time delay depends on many factors, which include the traveling transmission rate from sender to the receiver as it will travel through the content provider to the application provider, after being able to travel to aggregator before reaching the carrier to the end-user. Figure 9(b) shows that the highest waiting time occurs for 6 secs while the least waiting time occurs for 2 secs. However, it is expected that the end-user (authorize owner) required a maximum waiting time of 6 seconds for text message delivery with an average waiting time of 3.6 seconds.

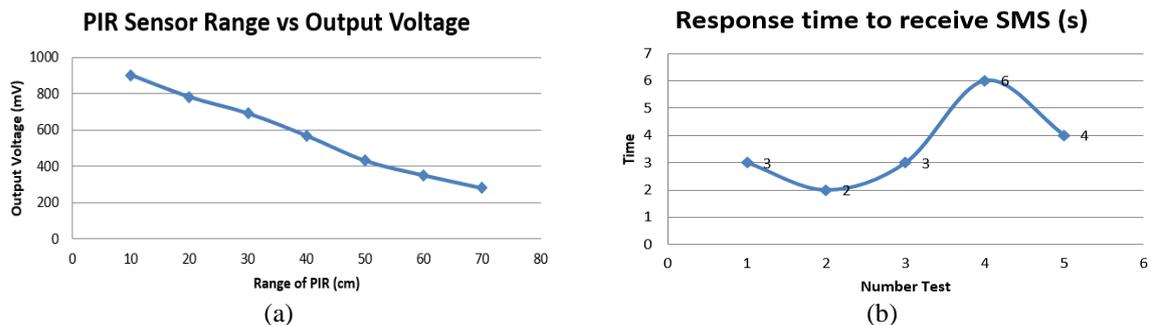


Figure 9. Experimental results, (a) Voltage vs. PIR sensor range and (b) Text messages received time

4.3. Generator load

The primary aim for load testing is to ensure that the micro-generator selected is suitable for powering low consumption power devices. In this testing LED's was utilized. Theoretically, a typical LED will consume approximately 20 mA and also required approximately 1.8 V to light up. Therefore, testing the power generated from the micro-generator will indicate that, the system has the capability to harvest energy that can store over time. In this test method, a voltage meter was utilized to measure current consumption to compare the measured power against the theoretical power consumption, power reading from the DC generator, and theoretical value. The system was tested utilizing 4 LEDs in four different stages so that the performance and efficiency of the developed energy harvest system can be measured, and setup perform with 4 LEDs, 3 LEDs, 2 LEDs, and 1 LED simultaneously. The voltage meter was utilized to measure current consumption to compare the measured power against the theoretical power consumption, power reading from the DC generator, and theoretical value shown in Figure 10.

The graphical analysis in Figure 10 describes the load analysis perform with 4 LEDs. The red line denotes the theoretical power consumption while the blue line is the measured powered measured using digital multi-meter; it can be observed that the system can generate enough power that can power low power consumption devices because it can power 4 or more LEDs.

4.4. Generator speed vs voltage

The testing performs to provide the selected DC generator's rotating speed against power generated by the DC generator. This testing is important to know the power that will generate whenever the sliding door is

in operation at a certain revolution per minute of DC generator. It also helps to understand how current generate, and amount of voltage generates for each testing. Two different data were collected: the voltage and current generated while the power was calculated by multiplying the voltage and the current together, generator speed tested between 75 rpm to 300 rpm. In contrast, the output current and voltage were monitored with a digital multi-meter. The results in Table 1 indicated that generator speed has the greater effect to power production because as the speed of the DC generator increase, this causes an increment of power generated range from 0.08 Watts to 1.13 Watts.

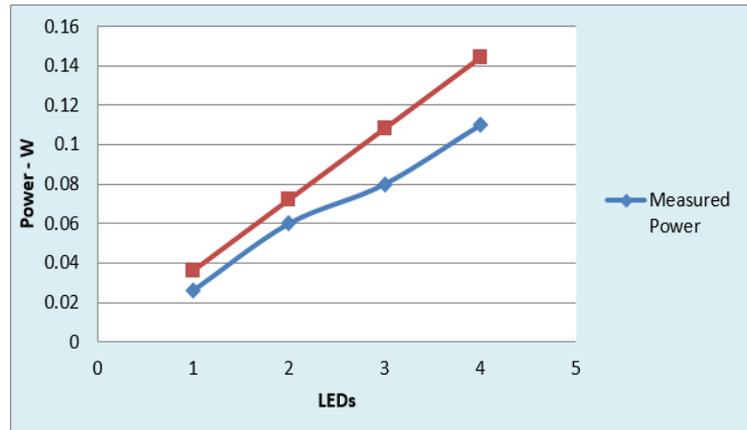


Figure 10. Comparison between measure and theoretical power generated by DC generator

Table 1. Generator speed vs voltage testing

Speed (rpm)	Current (A)	Voltage (V)	Power (Watts)
300	0.385	2.929	1.128
200	0.433	1.909	0.827
150	0.505	1.555	0.785
100	0.577	0.500	0.283
75	0.602	0.135	0.081

5. CONCLUSION

The current smart security door energy harvest system has been designed and developed, and further investigated to conclude. The investigation includes different ways that house security can achieve various patterns to utilize a rotational motion to generate electricity. The obtained results show much reliability in terms of its range covered and SMS delivery time with the expectation of not more than 6 seconds where it is not a substantial waiting time to access a room or house. The current study is a multi-purpose system which can utilize in many environments ranging from home, offices, shopping mall, hospital, hotel, and other section that their focus is to improve the security of conventional open and close door and to take advantage of this open and close to generate electricity from it.

The proposed study has a few limitations observed during implementation like the system do not generate expectation energy since most user open and close door will do it their way, some will open fast, allowing the DC generator to generate more energy while some will be very slow. Therefore energy or power generated varies from one time to another. Another limitation is the single method identification approach. However, this method was approach nicely because password generated is automatic, and it changes from time to time, though the authors believed that have multi-identification will increase the security compare to its initial security status. For future work, a fingerprint will be added to the door to provide maximum password security. Mobile application energy harvest and security monitoring can be introduced to remotely monitor a mobile application like Android APP and IOS. Finally, attaching a camera to the system will help identify the person who stands up in front of the door and send the SMS to the propriety owner.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

REFERENCES

- [1] Faisel, Z. G., Hussein, M. S. and Abood, A. M., "Design and realization of motion detector system for house security," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 17, no. 6, pp. 3211-3217, 2019.
- [2] Albak, L. H., Hamed, A. and Al-Nima, R. R. O., "Design Security System based on Arduino," *The Mattingley Publishing Co., Inc.*, 2020.
- [3] Chaurasia, A., Dwivedi, U. K., Chaurasia, A. and Jain, S. K., "A New Approach to Smart Knock Detection Based Security System for Door Lock," In *International Conference on Intelligent Computing and Smart Communication 2019*, 2020, pp. 907-914.
- [4] Rahman, M. M., Ali, M. S. and Akther, M. S., "Password Protected Electronic Lock System for Smart Home Security," *International Journal of Engineering Research and Technology*, vol. 7, no. 4, pp. 541-544, 2018.
- [5] Yang, J. C., Lai, C. L., Sheu, H. T. and Chen, J. J., "An intelligent automated door control system based on a smart camera," *Sensors*, vol. 13, no. 5, pp. 5923-5936, 2013.
- [6] Sarp, B. and Karalar, T., "Real time smart door system for home security," *International Journal of Scientific Research in Information Systems and Engineering (IJSRISE)*, vol. 1, no. 2, pp. 121-123, 2015.
- [7] Aman, F. and Anitha, C., "Motion sensing and image capturing based smart door system on android platform," In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 2346-2350.
- [8] Hussein, N. A. and Al Mansoori, I., "Smart door system for home security using raspberry pi3," in *2017 International Conference on Computer and Applications (ICCA)*, 2017, pp. 395-399.
- [9] Rahman, M., Zaman, M. and Mahmud, M., "Smart Lock System with Bio-metric Authenticity and Wireless Controlling," *DSpace Repository*, 2019.
- [10] Vinoj, V., Shaifee, C. D., Mafila, B. N. And Ashmi, S. B., "Voice Recognition Door Access Control System," *Purakala with ISSN 0971-2143 is an UGC CARE Journal*, vol. 31, no. 4, pp. 2140-2146, 2020.
- [11] Tshomo, K., Tshering, K., Gyeltshen, D., Yeshi, J. and Muramatsu, K., "Dual Door Lock System Using Radio-Frequency Identification and Fingerprint Recognition," in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, 2019, pp. 1-5.
- [12] De Lima, A. B., Gurung, B. and Farhad, S. M., "Efficient App Based Smart Door Lock System Using Bluetooth," In *Workshops of the International Conference on Advanced Information Networking and Applications*, 2020, pp. 1046-1055.
- [13] Yoon, S. H., Lee, K. S., Cha, J. S., Mariappan, V., Young, K. E., Woo, D. G *et al.*, "IoT Open-Source and AI based Automatic Door Lock Access Control Solution," *International Journal of Internet, Broadcasting and Communication*, vol. 12, no. 2, pp. 8-14, 2020.
- [14] Mitcheson, P. D., Green, T. C., Yeatman, E. M. and Holmes, A. S., "Architectures for vibration-driven micropower generators," *Journal of microelectromechanical systems*, vol. 13, no. 3, pp. 429-440, 2004.
- [15] Yeatman, E. M., "Energy harvesting from motion using rotating and gyroscopic proof masses," *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, vol. 222, no. 1, 2008, pp. 27-36.
- [16] Toh, T.T., Mitcheson, P.D., Holmes, A.S. and Yeatman, E.M., "A continuously rotating energy harvester with maximum power point tracking," *Journal of Micromechanics and Microengineering*, vol. 18, no. 10, 2008, Art. no. 104008.
- [17] Partridge, J. S. and Bucknall, R. W. G., "Potential for harvesting electrical energy from swing and revolving door use," *Cogent Engineering*, vol. 5, no. 1, 2018, Art no. 1458435.
- [18] Meshram, P., Kasurkar, A. and Pullawar, P.V., "Development in Energy Harvesting System Using Escalator and Four Way Door Mechanism," *International Journal of Advanced Research in Science, Engineering and Technology*, vol. 4, no. 4, 2017.
- [19] Ahamed, R., Rashid, M.M., Islam, J., Javed, A. and Yusof, H. M., "Energy generation from revolving door," *Indian Journal of Science and Technology*, vol. 9, no. 19, pp. 1-6, 2016.
- [20] Ryu, H., Yoon, H. J. and Kim, S. W., "Hybrid energy harvesters: toward sustainable energy harvesting," *Advanced Materials*, vol. 31, no. 34, 2019, Art. no. 1802898.
- [21] M. C. Hamilton, "Recent Advances in Energy Harvesting Technology and Techniques," in *38th Annual Conference on IEEE Industrial Electronics Society (IECON)*, 2012, pp. 6297-6304.
- [22] Bajrang, C., Suganthi, G. V., Tamilselvi, R., Parisabeham, M. and Nagaraj, A., "A Systematic Review of Energy Harvesting from Biomechanical Factors," *Biomedical and Pharmacology Journal*, vol. 12, no. 4, pp. 2063-2070, 2019.
- [23] Dong, L., Closson, A. B., Jin, C., Trase, I., Chen, Z. and Zhang, J. X., "Vibration-Energy-Harvesting System: Transduction Mechanisms, Frequency Tuning Techniques, and Biomechanical Applications," *Advanced Materials Technologies*, vol. 4, no. 10, 2019, Art. no. 1900177.
- [24] M. S. Murthy, Y. S. Patil, S. V. K. Sharmaa, B. Polem, S. S. Kolte, and N. Doji, "Revolving Doors Producing Green Energy," in *First Conference on Clean Energy and Technology (CET)*, 2013, pp. 157-160.
- [25] Sadeque Reza Khan, Ahmed Al Mansur, Alvir Kabir, Shahid Jaman, Nahian Chowdhury., "Design And Implementation Of Low Cost Home Security System Using Gsm Network," *International Journal of Scientific & Engineering Research*, vol. 3, no. 2, pp. 1-6, 2012.
- [26] Nafi, K. W., Kar, T. S. and Hoque, S. A., "An advanced door lock security system using palmtop recognition system," *International Journal of Computer Applications*, vol. 56, no. 17, pp. 18-26, 2012.

- [27] S. Ramesh, Soundarya Hariharan and Shruti Arora, "Monitoring And Controlling Of Bank Security System," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 10, 2012.
- [28] Agarwal, N. and Nayak, S. G., "Microcontroller based home security system with remote monitoring," *International Journal of Computer Applications*, pp. 38-41, 2012.
- [29] Chao-Huang Wei and Shin-An Chen., "Video Door Phone Surveillance System Using Powerline Communication Channel," *International Journal of Computer and Electrical Engineering (IJECE)*, vol. 5, no. 4, pp. 419-423, 2013.
- [30] Gangi, R. R. and Gollapudi, S. S., "Locker opening and closing system using RFID fingerprint password and GSM," *International Journal of Emerging Trends and Technology in Computer Science*, vol. 2, no. 2, pp. 110-115, 2013.
- [31] Muneer, A. and Fati, S. M., "Automated Health Monitoring System Using Advanced Technology," *Journal of Information Technology Research (JITR)*, vol. 12, no. 3, pp. 104-132, 2019.
- [32] Fati, S. M., Muneer, A., Mungur, D. and Badawi, A., "Integrated Health Monitoring System using GSM and IoT," In *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1-7.
- [33] Al-nabhani, S. and Muneer, A., "Automated library system using SMS based pick and place robot," *International Journal of Computing and Digital Systems*, vol. 8, no. 6, pp. 535-544, 2019.
- [34] Litwhiler, D. H. and Gavigan, T. H., "A Low-Power Instrumentation and Recording System for Swing Door Usage Analysis," *Engineering Technology Opens the Door to a World of Opportunity*, 2008.
- [35] Büren, T. V., Lukowicz, P. and Tröster, G., "Kinetic energy powered computing-an experimental feasibility study," In *Proceedings of the 7th IEEE International Symposium on Wearable Computers*, 2003.
- [36] Ahamed, R., Rashid, M. M., Islam, J., Javed, A. and Yusof, H. M., "Energy generation from revolving door," *Indian Journal of Science and Technology*, vol. 9, no. 19, pp. 1-6, 2016.
- [37] I. Syam Krishna, and J. Ravindra, "Design and Implementation of Home Security Sytem based on WSNS and GSM Technology," *International Journal of Engineering Science and Technology*, pp. 139-142, 2014.
- [38] Chaitanya Rane., "Password Based Door Locking System Using GSM," *International Journal of Engineering Trends and Applications (IJETA)*, vol. 2, no. 4, pp. 48-53, 2015.
- [39] Ogrı, U. J., Okwong, D. E. B. and Etim, A., "Design and construction of door locking security system using GSM," *International Journal of Engineering and Computer Science*, vol. 2, no. 7, pp. 2235-2257, 2013.
- [40] Eseosa, O. and Promise, E., "GSM based intelligent home security system for intrusion detection," *International Journal of Engineering and Technology*, vol. 4, no. 10, pp. 595-605, 2014.
- [41] Oke, A. O., Olaniyi, O. M., Arulogun, O. T. and Olaniyan, O. M., "Development of a microcontroller-controlled security door system," *The Pacific Journal of Science and Technology*, vol. 10, no. 2, pp. 398-403, 2009.
- [42] Kamelia, L., Noorhassan, A., Sanjaya, M. and Mulyana, W. E., "Door-automation system using bluetooth-based android for mobile phone," *ARNP Journal of Engineering and Applied Sciences*, vol. 9, no. 10, pp. 1759-1762, 2014.