DUJASE Vol. 5(1 & 2) 67-73, 2020 (January & July)

A Cost-Effective Security System for Smart Homes

Monisha Mushtary Uttsha, A.K.M. Nadimul Haque, Shamim Ahmed Deowan*, Sejuti Rahman

Department of Robotics and Mechatronics Engineering, University of Dhaka, Dhaka-1000, Bangladesh

**E-mail: shamimdeowan.rme@du.ac.bd*

Received on 21 June 2020, Accepted for publication on 10 September 2020

ABSTRACT

With the advancement of science and technology life has become simple and easy, but at the same time, lack of security has become a major problem in the day to day life. This paper focuses on the possible security threats on a lock and weighs them against the increasing cost and the possible solutions for overcoming them and proposes a smart security lock for simple home security application. In the proposed system, the owner gets the option to create and choose his own password, or reset the password. If the wrong password is given 25 times, an alarm will ring. If someone tries to break the lock forcefully, the excess pressure will be sensed and an alarm will ring. The low-cost but effective piezoelectric sensor, along with other low-cost devices make the proposed system cost effective and affordable, compared to other state-of-the-art systems.

Keywords: Piezo-disk, Vibration, Home security, Alarm, Safety, Lock.

1. Introduction

With the growing concern for home security, a smart and low-cost security system for general home security is becoming more important day by day, especially in developing countries like Bangladesh. Numerous cases of breaking and entering of homes, with intentions to rob and kill have occurred. Due to congested homes, large population and comparatively insufficient number of police, safety in our country is one of the biggest concerns for the general public. But to ensure safety, there is little to do for the middle-class citizens, as the rather high-end security locks are very expensive, and too complex to be mounted at residential homes. State-of-the-art security systems like biometric security systems start from 17,500 Taka [1], which is way too much for the middle-class citizens. Even password protected security systems such as [2], [3], [4] etc. are retailed at more than three thousand Taka, which is way too much for the huge middle-class population even in urban areas of Bangladesh. Not only that, but these systems do not provide any security regarding the lock itself, or the surrounding area it is mounted on.

This makes them vulnerable to breaking and enterings. That is why, to build a cost friendly and efficient smart security system that provides additional security to the lock itself as well as the surrounding area, has been the motivation of this work and piezoelectric materials play a key part in this.

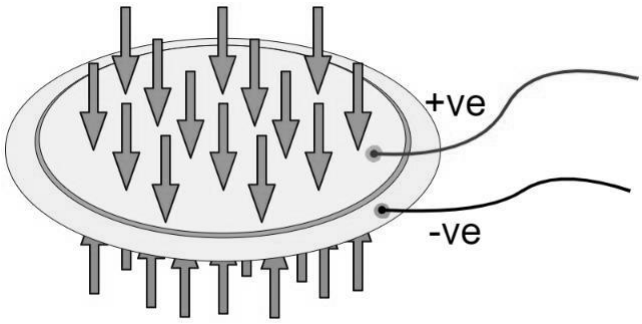

Fig. 1: Piezoelectric Sensor

Piezoelectricity has been used in the past few decades in various aspects in order to turn mechanical systems into electro-mechanical or totally electrical systems. Piezoelectric effect is the ability of certain materials to generate electricity when exposed to some mechanical stress. Thus, piezoelectric materials can easily be used to sense pressure. Piezoelectric sensors are mainly active sensors with some piezoelectric material on its surface.

When external pressure is given, an output voltage is generated (Fig. 1) [5]. The voltage can be measured using a voltmeter as it can be seen in the Fig. 2, and the change in voltage can be applied as a control mechanism.

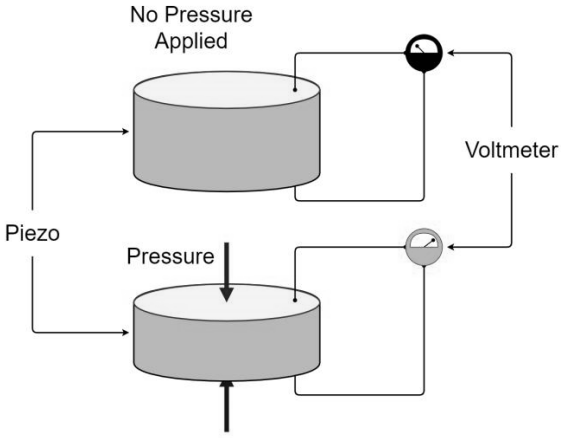

Fig. 2. Pressure sensing method of piezoelectric sensor.

Taking advantage of this phenomena, this paper proposes a security lock that is cheap, efficient, easily mountable in resident homes that not only ensures that no one can bypass or pick the lock, but also sounds an alarm by sensing the excess pressure using a piezoelectric sensor. The proposed security system, unlike other security systems on the market, detects excess pressure on any part of the door through the help of a piezoelectric sensor as well as triggering an alarm. The rest of this paper is organized as follows. Section II discusses some of the existing smart security systems. Section III discusses the materials used

and the design of the system. It also sheds light on the implementation details, the experimental settings along with the results. Finally, section IV concludes the paper by discussing the limitations of the system and the future works.

2. Literature Review

A. RFID and Biometric Security System

Park et al. [6] invented a digital door lock that also acted as the central controller of their system. Their system was an interconnected network of sensor nodes and actuators that has the digital door lock as the base station. Their lock consisted of Radio Frequency Identification (RFID) reader used for user authentication, a touch LCD for inputs and visuals, motor module for door opening and closing, and also sensor modules used for detecting the condition of the interior of the house. However, the system lacked the counter measure in case someone tries to break the lock or controller. Keogh and Keogh [7] invented a biometric lock system that recognized fingerprint pattern. It used a fingerprint sensor for detecting the fingerprint, a memory device that stored the fingerprint data, a verifying unit that verified the fingerprint input to the ones stored on the memory unit and a motor control unit that opened the lock. When the current fingerprint input matched with a fingerprint already enrolled, the motor control unit is supplied a direct current to open the lock. This system was very efficient, but out of reach for even higher middle-class citizens. One rather inexpensive lock system developed by Verma and Tripathi [8] used the RFID technology that functions without a battery. It used a passive tag that verified and authenticated the user and unlocked the door, all happening in real time. This system was both cheap and useful. However, it lacked the counter measure for someone trying to break the lock. It also failed in the aspect that if the tag is lost, then even the real owner might be locked out. It might also be prone to hacking into the lock.

B. Wireless Security System

Shaikh et al. [9] used near field communication chip (NFC) in smartphones to regulate the lock opening mechanism. Access was regulated using NFC smart card. This allowed an administrator to grant or deny entry to a particular user. Every NFC smart card had a unique identification. This was used in this project for allowing access. This method was very clever, cheap and efficient. This was built to be available to middle-class citizens.

However, this required a smartphone to be carried by the administrator. So if the user forgot to carry the smartphone or somehow loses it, he would not be able to open the lock. Authors in [10], proposed a remote home security alarm system by creating a wireless sensor network (WSN) and integrating GSM (Global System for Mobile Communications) technology. Their system could detect robberies, gas leaks, fire etc. and send an alarm message remotely to the owner. This type of implementation is efficient, but costly. They also incorporated aspects that are out of the scope of this paper. Maato et al. [11] proposed fingerprint based security system using LabVIEW. This used the fingerprint as a pass code for the lock system and a red LED light and an alarm for any kind of hacking. Though this was a low cost system, it do not produce any alarm or warning when someone tried to break the lock manually. Moreover, if anyone hit on the surface of the door apart from the lock and tried to break in, it would not start any alarm. Isa et al. [12] proposed a system that used keypad to enter password and GSM module for sending message to the owner or central security in charge. Also, a camera and a speaker were used to capture the photo of the person giving wrong passcodes and for an alarm sound respectively. But again, this system lacked the features of giving alarm or other kinds of signal to a manual break in, unlike hacking the security systems software. Also, it was costlier and needed additional memory to store the images. J. Chandromohan et al. [13] proposed a system both for security purpose and home automation using wifi and an android application. However, depending only on a wifi network made the security system vulnerable to hacking. Lakshmi et al. [14] proposed another system that used image recognition and motion sensor. It took photo of a person who came in front of the lock and compares the photo with an already stored image. The drawbacks for this system were that it needed a good resolution camera which made this system quite an expensive one.

Again, any kind of change of appearance could create problem to recognize a person. Both memory and cost of the system also create problem.

C. IoT and Security System

Another system for home security, proposed by Assaf et al. [15] used field programmable gate array (FPGA) for their system. It uses IoT that enables users to interact with the system through internet. Abu et al. [16] also proposed a similar approach using IoT. But they also used Passive Infrared sensor, Infrared sensor and Blynk application. Although these systems offered a user-friendly security system, in case of any kind of hacking or break in these only send message to the owner via email. So, if internet connection became unavailable to the owner at that moment, they would not get the alert on time. Another IoT based home security system by R.K. Kodali et al. [17] proposed to use Passive Infrared (PIR) sensor to detect trespassers and also a warning message to the owner to take further action would be sent. However, since it only detected motion, it could not differentiate between an intruder and other people which makes it less efficient. Song et al. [18] proposed a surveillance robot which was equipped with hopping capabilities for security purposes specially for residential area. The robot used ZigBee protocol for wireless communication. Although this was an innovative and exciting idea, and possibly quite effective as well, this was very expensive and not possible for middle class citizens to buy this. Luo et al. [19] proposed a multiple remote interface security system (MRISS) which was integrated with intelligent security robot (ISR). It also used security supervise computer, RF interface, GSM module and other

appliances for the control module. Through MRISS, they intend to control all the appliances as well as detect any abnormal or dangerous situations and send message via GSM module. Even though this system could address the issue of any type of threat, this was very costly.

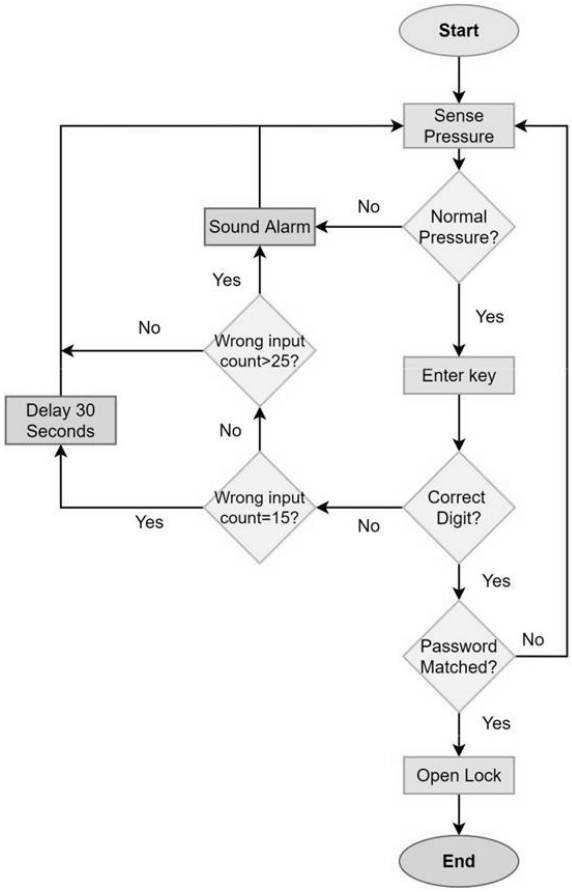

Fig. 3. Flowchart of the algorithm

D. Piezoelectricity and Security System

Piezoelectric sensors have been used by many researchers. Face [20]created an anti-braking system that utilizes the piezoelectric effect. The braking system includes a highly controllable pre-stressed piezoelectric element. Compared to other braking systems that were driven by a mechanical system, using slip sensors and piezoelectric element, the braking system is driven by an electrical system. Piezoelectricity has also been used in locking mechanisms. Conforti [21] created a low battery consuming wireless access control system that used piezoelectric locking mechanisms. However, this application only offered a locking mechanism. It did not provide any security options.

It can be clearly understood that even though there are smart security systems available, those often are very complex and expensive and cannot be afforded by the general public. Also, most of the works provide security only of the lock, and not where it is mounted on. Our system not only offers security of the locking mechanism, but also the surrounding area it is mounted on, e.g. the door, making breaking and entering, that much more difficult.

3. Materials and Methods

Piezoelectricity is the electric charge generated in certain materials when stress is applied on its surface. Although the generated voltage is too little to be used anywhere, it can be easily measured. The applied pressure can also be found from the measured voltage as well. However, rather than finding the exact pressure applied, finding the range of voltages that are generated from different pressures is easier and faster to compute, thus proves to be more useful. This, combined with the cheap and readily available quartz piezoelectric sensors or piezo disk as seen in Fig. 1, built the foundation of this work. This section first discusses the design and layout of the system. Then we move onto the material selection where we briefly discuss about the materials chosen.

A. System Design

The security system has a microcontroller set up with the lock. Piezoelectric sensor is used to determine the force put upon it. The pressure is calibrated in a manner so that when normally the keys are pressed, it will be counted as the security code, but pressure higher than a certain amount, signals the possibility of a break in. This, in turn, activates an onsite alarm to warn the residents at home. The alarm turns off only if the correct password is given. However, if the pressure is normal, it is counted as a security code and this is matched with the already confirmed and set code stored in memory of the microcontroller. The lock uses a stepper motor that will rotate a certain degree to open the lock. The lock automatically closes after 30 seconds. If someone is giving wrong inputs again and again, the keypad stops taking input for 30 seconds after 15 wrong inputs. From thereon, if 10 more wrong inputs are given, the alarm is activated that will only turn off if the correct password is given. With the system design in place a working principle for the security system can be developed as shown in Fig. 3.

B. Device/Material Selection

The main criteria for the material selection were availability, low cost and high performance. These materials are mostly meant for only the prototype. But for the actual product, many of the hardware need to be replaced with more rigid materials. With that being said, the following devices and materials were selected-

1) Arduino UNO - This is a microcontroller board developed by Arduino.cc equipped with an 8-bit AVR microchip. This acts as the main controller of the whole system by constantly communicating with all the connected components.

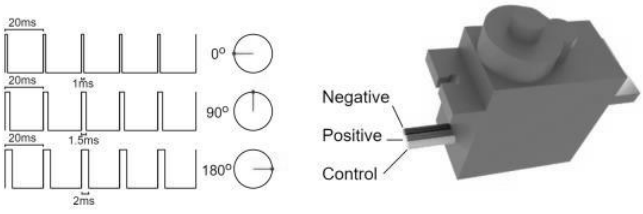

Fig. 4. SG90 Micro Servo Motor

2) SG90 micro servo motor - It can be easily controlled to rotate at a specific angle with sufficient accuracy as shown in Fig. 4. With a bar connected to its shaft, it makes up our prototype lock that serves our purpose for this work. The controller dictates upon which conditions the servo motor is to rotate to open or close the lock using the control wire of the motor.

3) 4x4 Matrix keypad - As the name suggests, the keypad has a total of 16 distinct characters, which make up the password. Pressing these keys act as the input of the passwords.

4) Buzzer - A buzzer is an audio signalling device. It works as the alarm system for this work.

5) Piezo disk - This is a type of piezoelectric sensor. It is used to sense the pressure put on the lock and door (can be seen in Fig. 2). Since our goal is to create a security system that unlike others, alerts the owners not only when someone tries to break the lock but also when someone tries to break the surface where the lock is attached to as well, a cheap but efficient sensor of this type was needed. Piezo disks are able to sense both the pressures created on the lock and even on surface of the door, as they can sense the vibration created on the surface due to the pressure and output a corresponding voltage.

6) PVC board - This is a lightweight rigid material that acts as the base of this system.

7) Connecting wires - These are jumper wires used to connect the components to the controller and power source.

8) Breadboard - Breadboard is a solderless device for temporary prototype circuitry. This acts as the hub of the circuit connections.

9) Prototype lock - This has been built using a bar like cutout from the PVC board, connected with the shaft of the servo motor. Although it is not very rigid or practical, it serves the purpose of this work.

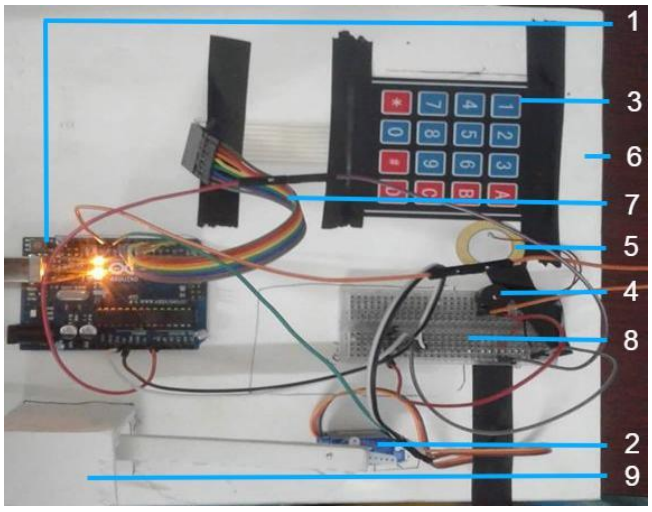

Fig. 5. Prototype of the system

The components can be seen on Fig. 5 with appropriate labels.

C. Implementation

1) Hardware Setup: We first needed to design and create a prototype lock to test our system on. For that, we attached a bar like extension to the servo motor and mounted it on a PVC board surface to simulate a lock on a door. We attached a piezo disk and a keypad along with the controller on the side of the surface. We added a buzzer with the controller circuit that we used as an alarm.

We connected all the components with the micro-controller so that we could design an efficient algorithm that would allow it to control the system properly.

2) Control Algorithm Creation: For the security system to work efficiently, we had to design a control algorithm that would make the system immune to hacking, sensitive to excess pressure in case of breaking and entering and easy to use for the general mass. Since our intentions were to create a password protected system, we had to be careful that no one can simply guess the password. For that we put a check upon each input for a match, i.e. it would check the password character by character rather than all at once at the end. And any mismatch would mean that the user would have to re-enter the password from the start. This would mean that the person entering the password would have to match every character from start to finish. Each wrong input will increment the error count. For 14 error counts, the user will be able to try again. However, after 15 counts, the user will not be able to give the password for the next 30 seconds. After that, the user will be allowed 10 more counts of errors. After the error count reaches 26, the alarm will ring alerting the owners of a possible security threat. The alarm can turn off only after the correct password has been given. This ensures that no one is able to keep on guessing the password hoping for a match. However, if that person is able to see their progress, i.e. how much they got right before they had to start over, they might be able to guess all the characters. That is why we did not attach a display to the system. The error count resets to 0 after the right password is given.

We then modified the algorithm to integrate the piezo disk so that it would be able to sense the pressure put not only on the lock, but also on the surface of the door as well. The controller would react and ring the alarm not only when excess pressure is put on the lock during password input, but also anytime it sensed excess pressure on the surface the lock is mounted on.

This meant that no one would be able to break neither the lock nor the door it is mounted on. We experimented extensively to find out the threshold value of the corresponding voltage due to excess pressure that would trigger the alarm.

D. Experimental Settings

The lock was initially tested with a set length of password to see if it works correctly. In this prototype of the proposed system, all the digits, four uppercase alphabets(A,B,C,D) and two special characters(*,#) have been used. Then the

lock was tested under different passwords, with various lengths and including characters. From these tests, the optimum tolerance level of 25 error counts was selected that allows the user to correct his or her mistakes, but that level is not nearly enough for someone to hack in by guessing the password. The idea of checking letter by letter also allows little room for error. This, however, also means that an intruder might be able to figure out the correct character in that position. To negate this possibility, the system uses a dummy length that only warns the user about him or her giving the wrong password after a certain amount of wrong inputs(15).

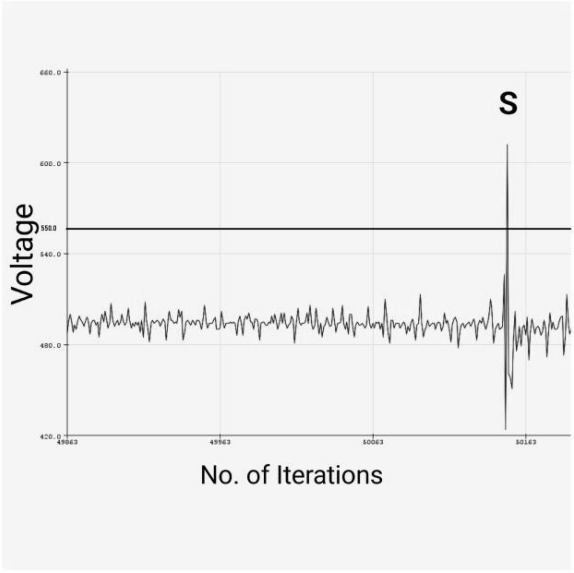

Fig. 6. Voltage change due to pressure on the lock. The bolded line denotes the equivalent threshold Arduino voltage. S denotes the voltage due to abnormal pressure.

The delay times were adjusted to allow the user to come in. To ensure that no one can break in, the piezo electric sensor was placed on the PCB board base. The sensor would sense the pressure put on the lock or anywhere on the base. To find the threshold value to detect a break-in, we tested with different amounts of pressure when giving the password, and noted the corresponding voltage. From Fig. 6, the voltage can be seen on each interaction with the lock. Each iteration and its corresponding voltage values show how much the pressure is put on the lock and its surface. We can see from the graph that during normal interactions such as button pressing, the pressure and the corresponding voltage is low. However, whenever we punched the lock or the PVC board it is mounted on, there is a huge spike on the voltage level denoting abnormal pressure and a possible threat. The threshold value (Denoted by the bold horizontal line in Fig. 6) was taken as the median of these extreme values. Pressure above the threshold value triggers an alarm created by the buzzer.

E. Result

Several inputs and consequent system responses were noted. They are shown in the TABLE I. We see that whenever the input password character differs from the set password, the cursor returns to the first character and looks to match it from the beginning and the error count increments by the number of wrong inputs given. We also see that as soon as the right password is given the servo motor operated prototype lock opens, it remains open for 10 seconds so that the user can pass. The lock gets automatically closed after 10 seconds and then remains locked until the user further gives the correct password. But when wrong keywords are given as password for more than 14 turns, the security system ignores any input given for the next 30 seconds. Furthermore, if the user again gives 10 more wrong inputs, an alarm buzzes that does not stop until the right password is given. Moreover, when someone tries to break the lock by putting excess pressure on it or on the the surface on which the lock is placed on, the alarm buzzes by sensing the pressure from the voltage change in the piezo disk connected with the system. And the alarm again, does not stop until the right password is given. So if anyone wants to break the lock the original owner will be alerted about the breaking by the sound of the alarm. As this system uses piezoelectric material to sense the pressure, the alarm buzzes even when the pressure is created on just the surface where the lock is placed on i.e. door, wall etc. This is possible because piezo disks can sense the vibration due to the pressure and a voltage change occurs. The voltage in Arduino is scaled to show voltage range of 0 to 5V as 0 to 1023. The actual voltage generated by the vibration in the piezo disk can be found from the equation-

$$\text{Voltage} = \text{Sensor value} * (5/1023) \quad (1)$$

Table 1. System Responses

Original Password	Keypad Input	Alarm State	Number of Error Keypad Input	State of Keypad	Lock
12AB	11345	Silent	4	Not Blocked	Closed
12AB	125AB	Silent	4+3=7	Not Blocked	Closed
12AB	09876	Silent	7+5=12	Not Blocked	Closed
12AB	345	Beep once	12+3=15	Blocked (for 30 second)	Closed
12AB	12AC	Silent	15+1=16	Not Blocked	Closed
12AB	23456	Silent	16+5=21	Not Blocked	Closed
12AB	51324	Silent	21+4=25	Not Blocked	Closed
12AB	2	Continuous Beeping	25+1=26	Not Blocked	Closed
12AB	12AB	Silent	0	Not Blocked	Open

The output signal from the piezo disk can be observed in Fig.-6. From the experiments, The range of values for normal pressure (the pressure created when the buttons of the keypad are pressed), Arduino Equivalent Voltage <= 550. Or, the actual voltage is, Voltage <= 550x(5/1023) <= 2.688 volts.

So, the threshold value for the system is 550 (Arduino Equivalent Voltage) or 2.688 volts(Originally). The alarm buzzes as soon as the voltage level goes above 550 or 2.688 volts, indicating abnormal pressure and a possibility of a break-in. So if someone even tries to break the door without touching the lock, the security system will sense it because of the corresponding voltage change in the piezo disk due to vibration and buzz the alarm, hence, alert the original owner. However, this may vary according to the rigidity of the lock or door. The system proved to be efficient and accurately detected excess pressure 100% of the time. The lock was provided to 20 selected people to be tested. They responded that the system seemed very useful to them and they were comfortable using it with more rigid hardware. 15% of them thought that a visual aspect would be better for displaying passwords, but others agreed that this no display feature added a new layer of security, further ensuring that the system is not easily hacked. Overall, the response was good from the test subjects.

A comparative analysis of cost between our system and some state-of-the-art electronic security systems available in Bangladesh is shown in Table-2. We found that biometric systems, although secure, is very expensive and so, out of reach for the middle-class citizens. The cheap password protected systems available on the market does not provide much security concerning hacking the system. Although the expensive ones do that, they provide no protection if someone tries to even cut the whole door in half. The motion detecting system of [22] is expensive like others of its kind. The cheaper versions are not accurate and adequate in such applications. Vision based automated security systems are not even available in the country. Even if they were, these systems are expensive and has a concern for memory and advanced facial recognition algorithms that drive up the cost way too much.

In comparison, our system, even without the piezo-electric sensor, performs adequately with an algorithm that makes it almost immune to hacking, and is comparable to the advanced password protected systems. However, with the piezo-electric sensor, it expands the security measures to the next level as the surrounding area is also taken under consideration for breaking and entering, offering total security. Whereas other systems, do not provide such counter measures with such low cost. And apart from all that, our system cuts the cost from the next cheapest, functional smart security system we could find on the market, more than 3 times. This is due to the cheap materials and sensors used for the minimal amount of hardware implementations and a stronger software side that compensates for that. Even in real world implementation, our valuation for the cost of creating the system is no more than 800 Tk. (200 for the lock, 300 for the controller, 200 for the power system and 100 for the sensors including the piezo disk), estimating retail at around 950 Tk. In contrast, other systems tend to drive up the price with expensive hardware and gimmicks that make the system more vulnerable to security threats whereas we included only the absolute necessary features and hardwares so that there remains that much less vulnerabilites. This approach make our system, fit for undercutting and taking over the market of smart security systems and allowing even middle class citizens, a much required feeling of safety.

Table 2: Comparative Cost Analysis Between Different Security Systems

Security Systems	Approximate Market Value (In Taka)	Type of the Security System
Xiaomi Mijia DGNWG02LM Multifunctional	3,500	Password Protected
Gateway Alarm System [3]		
Everspring SC423 Wireless Security Alarm [2]	12,000	Password Protected
Cop Security 15-946 Motion Detector Sensor Se-	4,700	Motion Sensing
curity Alarm [22]		
ZKTeco TL100 Anti-Theft Fingerprint Lock with	17,500	Biometric Based
Touch Keypad [1]		
Password Protected L220 Digital Locker Vault [4]	14,500	Password Protected
Our System	950	Password Protected

4. Conclusion

We proposed a security system which is both cost effective and efficient, capable of addressing the market for cheap security systems in developing countries. The system takes password input from the users and matches it with the existing password character by character. Such character by character matching lessens the risk of simply guessing the password. The alarm system ensures that no one can keep guessing and eventually land on the right password, even though the character by character matching ensures the probability of that is very low. The absence of a visual aid also helps with that as hackers get no indication whether they are guessing right or wrong, until of course, it is too late and the system stops taking input with only a few tries left before the alarm starts ringing. The system also allows the user to turn off the alarm by giving the right password.

Currently, the system only sounds an alarm that can be heard if the owner is in the house or nearby. If the owner is away, there is no way to alert him. This can be solved by adding a GSM shield to send the message to owner and perhaps the police as well. Even though it will cost more, it may be added to higher end products. Using rather cheap materials allow more flexibility to adding more features if necessary, all the while keeping the price in range of the

targeted middle class customers. Future works can be done in integrating it with other home appliances to form an interconnected network. It can also be made to be wireless. However, the security protocols have to be maintained strictly and carefully so it is not hacked. Thus, the cost would increase. That is why the current wired system is proposed. The system can also be modified using a wireless communication device to establish an interconnected security system in large buildings. The central controller will communicate with various local systems to gain and use information about the area of break in to instantaneously take action.

References

1. "Zkteco tl100 anti-theft fingerprint lock with touch keypad," Aug 2020. [Online]. Available: https://www.bdstall.com/details/ zkteco-tl100-anti-theft-fingerprint-lock-with-touch-keypad-44383/
2. "Everspring usc423 gsm wireless alarm system," Aug 2020. [Online]. Available: https://www.bdstall.com/details/ everspring-usc423-gsm-wireless-alarm-system-38907/
3. "Xiaomi mijia dgnwg02lm multifunctional gateway alarm system," Mar 2020. [Online]. Available: https://www.bdstall.com/details/xiaomi-mijia-dgnwg02lm-multifunctional-gateway-alarm-system-47146/
4. "Password protected l220 digital locker vault," Dec 2019. [Online]. Available: https://www.bdstall.com/details/ password-protected-l220-digital-locker-vault-47946/
5. G. Gautschi, "Piezoelectric sensors," in Piezoelectric Sensorics. Springer, 2002, pp. 73–91.
6. Y. T. Park, P. Sthapit, and J.-Y. Pyun, "Smart digital door lock for the home automation," in TENCON 2009-2009 IEEE Region 10 Conference, 2009, pp. 1–6.
7. C. Keogh and K. Keogh, "Fingerprint biometric lock," Jul. 31 2003, US Patent App. 10/358,013.
8. G. K. Verma and P. Tripathi, "A digital security system with door lock system using RFID technology," International Journal of Computer Applications, vol. 5, no. 11, pp. 6–8, 2010.
9. I. Shaikh, S. K. Chilukuri, and B. Tejaswi, "Security system using Raspberry Pi with door lock controller," International Research Journal of Engineering and Technology, vol. 5, no. 3, 2018.
10. H. Huang, S. Xiao, X. Meng, and Y. Xiong, "A remote home security system based on wireless sensor network and GSM technology," in 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 535–538.
11. J. Maato, E. Mwangi, and P. M. Karimi, "A low cost computer based fingerprint security system for restricted access control automation using LabVIEW," International Journal of Computer Applications, vol. 163, no. 8, 2017.
12. E. Isa and N. Sklavos, "Smart home automation: GSM security system design & implementation." Journal of Engineering Science & Technology Review, vol. 10, no. 3, 2017.
13. J. Chandramohan, R. Nagarajan, K. Satheeshkumar, N. Ajithkumar, P. Gopinath, and S. Ranjithkumar, "Intelligent smart home automation and security system using Arduino and Wi-Fi," International Journal of Engineering And Computer Science (IJECS), vol. 6, no. 3, pp. 20 694– 20 698, 2017.
14. R. Lakshmi, P. L. Priya, G. Lokanyaa, and J. J. Sharmila, "Security system using Raspberry Pi with door lock controller," International Journal of Engineering Science and Computing, vol. 7, no. 4, 2017.
15. M. H. Assaf, R. Mootoo, S. R. Das, E. M. Petriu, V. Groza, and S. Biswas, "Sensor based home automation and security system," in 2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings, 2012, pp. 722–727.
16. M. A. Abu, S. F. Nordin, M. Z. Suboh, M. S. M. Yid, and A. F. Ramli, "Design and development of home security systems based on internet of things via favoriot platform," International Journal of Applied Engineering Research, vol. 13, no. 2, pp. 1253–1260, 2018.
17. R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," in 2016 international conference on computing, communication and automation (ICCCA). IEEE, 2016, pp. 1286–1289.
18. G. Song, K. Yin, Y. Zhou, and X. Cheng, "A surveillance robot with hopping capabilities for home security," IEEE Transactions on Consumer Electronics, vol. 55, no. 4, pp. 2034–2039, 2009.
19. R. C. Luo, T. Hsu, T. Lin, and K. Su, "The development of intelligent home security robot," in IEEE International Conference on Mechatronics, 2005. ICM'05. IEEE, 2005, pp. 422–427.
20. S. A. Face Jr, "Anti-lock brake system with piezoelectric brake actuator," Apr. 10 2001, US Patent 6,213,564.
21. F. J. Conforti, "Wireless access control system with energy-saving piezo-electric locking," Jun. 29 2010, US Patent 7,747,286.
22. "Cop security 15-946 motion detector sensor security alarm," Aug 2020. [Online]. Available: https://www.bdstall.com/details/ cop-security-15-946-motion-detector-sensor-security-alarm-30747