iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34515

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Tamper Proof Embedded Hardware for Secured Applications

Abhishek Katragadda[1], Saragada Puneeth[2], AVS Sai Teja[3], Dr. J. Chattopadhyay[4]
[1, 2, 3]*Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad*
[4]*Professor. Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad*

Abstract: ***An embedded hardware designed for critical application like defence, health and industry application requires to be secured. The system may be subjected to masquerading, eavesdropping and denial of service. This can be done in several ways. One of the common modes is by tampering the hardware through physical access or memory corruption through external attack. In order to mitigate this, it is necessary to design a tamper proof hardware. Whereby, in case of intrusion the same can be communicated to the owner and preventive actions can be taken. This can be done by adding sensors to the box to monitor its physical status and then the status can further be transferred through IOT***
Keywords: Tamper proof, embedded, secured application, intrusion, IOT

I. INTRODUCTION

Security has become a major concern in this fast-paced world especially embedded system security. Nowadays embedded systems are being used for storing the data and it is also being used as a lock to protect some physical objects. An embedded system as a lock has a great significance in our day-to-day life as it protects the valuables of its users from intruders. These embedded systems have to be designed in such a way that they don't give access to an unknown person and they have to withstand with the physical damages and software tampering done by the intruder. The main purpose of using embedded system as a lock is that they provide three major features like confidentiality, integrity and availability. Confidentiality lets the user to not give access to an unknown person and keeps the information private. Integrity doesn't let any unknown person to access information or to overwrite the information present inthe embedded system. Availability lets its users to access the information when needed without any delay and provides the same information to the user which was previously stored by him in the system. These three features enables the user to prevent the system from being tampered and from virus attacks. The attacks are also physical in nature and that leads to the tampering by opening the lid etc. In this paper, we have proposed a method that protects the system from physical attacks like box opening or damaging etc. This also has necessary protection for a known user to use the system. It looks for an user interface which when connected ask for a password/ OTP and authenticate the user. Thereby the system will stop alert generation. This feature can be enabled or disabled. There are very few literatures available in this direction which will be discussed below. Subsequently we will discuss about the methodology and also the hardware and software components used for this. Several applications of this product are discussed subsequently. At the end we conclude with future works.

II. LITERATURE SURVEY

The use of tamper resistance in cryptography goes back for centuries. Naval code-books have been weighted so they could be thrown overboard and sink in the event of imminent capture; to this day, the dispatch boxes used by British government ministers' aides to carry state papers are lead-lined so they will sink. Codes and, more recently, the keys for wartime cipher machines have been printed in water-soluble ink. To overcome such the need to develop the electronic devices, as well as some mechanical ciphers, were built so that opening the case erased the key settings. Following a number of cases in which cipher staff sold key material to the other side. So, engineers started paying more attention to the question of how to protect keys in transit as well as in the terminal equipment itself. The goal was 'to reduce the street value of key material to zero', and this can be achieved either by tamper resistant devices from which the key cannot be extracted, or tamper evident ones from which key extraction would be obvious. Paper keys were once carried in tattle-tale containers, designed to show evidence of tampering. When electronic key distribution came along, a typical solution was the "fill gun," a portable device that would dispense crypto keys in a controlled way. Nowadays, this function is usually performed using a small security processor such as a smartcard. Control protocols range from a limit on the number of times a key can be dispensed, to mechanisms that use public key cryptography to ensure that keys are loaded only into authorized equipment.

The control of key material also acquired broader purposes. In both the United States and Britain, it was centralized and used to enforce the use of properly approved computer and communications products.[2] Live key material would only be supplied to a system once it had been properly accredited. Once initial keys have been loaded, further keys may be distributed using various kinds of authentication and key agreement protocols. So, by studying the current technologies we thought there is a need for developing an OTP based lock which provides more security to the valuable than the existing technologies.[1]

III. WORKING

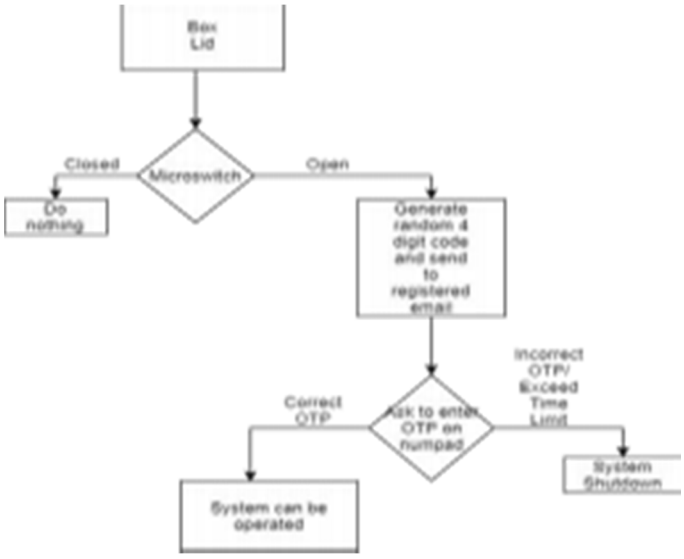
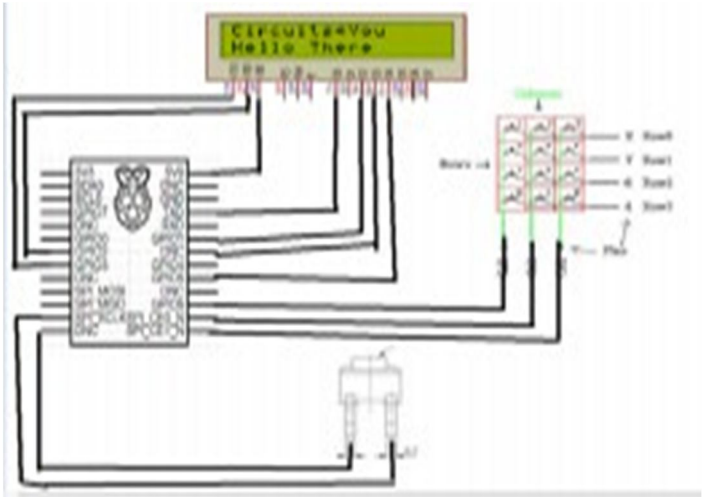


Fig 1. Flow Chart of Working Model

This set up initially relies on a microswitch to learn about the status of the box. The microswitch is connected to the Raspberry Pi which regularly reads the state of the switch. The switch being in a closed state indicates that the box is closed while the switch in open state indicates that the box is open. Once the Raspberry Pi learns that the box is open, a random four-digit number is generated and sent to a registered email address. As soon as the code is sent, a timer for one minute begins. The code can be entered using the 4x4 keypad. Once 'A' is pressed on the keypad, the values entered prior to this action are read and compared to the random digit that is generated. If the code entered is correct, the system exits this process and allows the user to use the system as normal. But, if the entered code is incorrect or the timer expires before the code can be entered, the system will lock out the user by force shutting down.

IV. CIRCUIT DESIGN



A. The common terminal of Microswitch is connected to the 5V terminal of Raspberry Pi.
B. The normally open terminal is connected to check the state of Microswitch.
C. The LCD is also given a 5V power supply.
D. The intensity of the LCD can be controlled using the potentiometer on the back.
E. The terminals on the keypad are connected to their respective rows and columns.
F. When a key is pressed, the row no. and column no. is sent as input to the Raspberry Pi.

V. HARDWARE AND SOFTWARE DESCRIPTION

A. Raspberry Pi

Fig 2. Raspberry Pi 3B+

Raspberry Pi is a very popular microcontroller, which is the size of a credit card. The variant being used here is Raspberry Pi 3B+. It has a dual core processor with 1 GB of RAM and multiple I/O ports, SPI (serial peripheral interface), and PWM (pulse width modulation) ports that can be used be used as per the required application.

B. Micro Switch

Fig 3. Microswitch

A Micro Switch is a small, very sensitive switch which requires minimum compression to activate. They are very common in-home appliances and switch panels with small buttons. Micro Switches have an actuator which, when depressed, lifts a lever to move the contacts into the required position. Microswitches often make a “clicking” sound when pressed this informs the user of the actuation.

C. 16x2 LCD

Fig 4. 16x2 LCD with HD44780 IC

LCD modules are very commonly used in most embedded projects, the reason being its cheap price, availability and programmer friendly. Its operating voltage is 4.7V to 5.3V. Further, the LCD should also be instructed about the position of the pixels. Hence it will be a hectic task to handle everything with the help of MCU, hence an Interface IC like HD44780 is used, which is mounted on the backside of the LCD Module itself. The function of this IC is to get the commands and data from the MCU and process them to display meaningful information onto our LCD Screen.

D. 4x4 Keypad Module

Fig 5. Keypad Module

In order to give input to the Raspberry Pi for accessing it we tend to use a keypad module. A 4x4 keypad will have eight terminals. In them four are rows of matrix and four are columns of matrix. These 8 pins are driven out from 16 buttons present in the module. Those 16 alphanumeric digits on the module surface are the 16 buttons arranged in matrix formation.

E. GMAIL

The OTP that is generated needs to be sent to the user for authentication purpose. Hence, this OTP will be sent to the pre-selected GMail address for verification.

F. SMTP (Simple Mail Transfer Protocol)

In this project the user is provided an OTP that has been randomly generated and sent to the user for verification in order to access the hardware. Hence, we use SMTP in order to accomplish this. SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet. It is a program used for sending messages to other computer users or devices based on e mail addresses.

VI. APPLICATIONS

A. ATM Machine

ATMs are convenient, they allow consumers to perform transactions with great ease. ATMs require the latest in technology because of the evolution of the machine from a single unit in a secure bank to a host of machines in stores, malls and markets. There are two types of locks used in the ATM machine. One is hardware locks. Even as physical security needs have increased, so have electronic security needs. Software encryption keys protect transaction records and prevent hackers from getting into an ATM.[3]

B. Smart Cards

The Smart Cards are pretty much self-reliant. This makes them resistant to attack as they do not need to depend upon potentially vulnerable external resources. This is one of the important reason why Smart Cards are often used in applications which require strong security protection and authentication. The smart Cards are provided with proper encrypted data.[4]

C. Smart Door

Electronic door locks are a way to automate the latest features like remote locking and unlocking. The electronic locking system accepts the signal as an input. This input can come in as different forms like Biometrics. This is a popular and secure method of allowing access to a lock. A small computer is installed on the lock itself. The scanner takes input and compares with the already stored data. If a person has access to the lock, a record of their biometric information will be found by the computer and it will send the release signal to the lock.[5]

VII.FUTURE SCOPE

The existing prototype discussed can prevent unauthorised access to the system, however it does not protect the data if the such unauthorised access does occur. Hence by adding or encrypting the user sensitive data we can protect the information as a second layer of protection. The password too is a numeric code but the combinations are still limited. Hence, the passwords too need to be more difficult to crack and if possible, use extra inputs such as finger prints or smart cards or a combination of all these to make tampering as difficult as possible.

VIII. CONCLUSION

In this paper we have discussed our approach to prevent tampering physically through the use of IoT. A method has been discussed for creating a tamper proof hardware, in this case a way to prevent unauthorised access to the Raspberry Pi. The prototype not only prevents the unauthorised use but also messages the user if any tampering has occurred based on the number of attempts.

We believe that a clear understanding of attacks as well as the trade-offs associated with deploying tamper resistance mechanisms will enable a system architect to develop a truly secure embedded system. We emphasize that there is no complete solution, and the major aim of this paper is to contribute positively (even a modest effort) on combating tampering of hardware.

IX. ACKNOWLEDGMENT

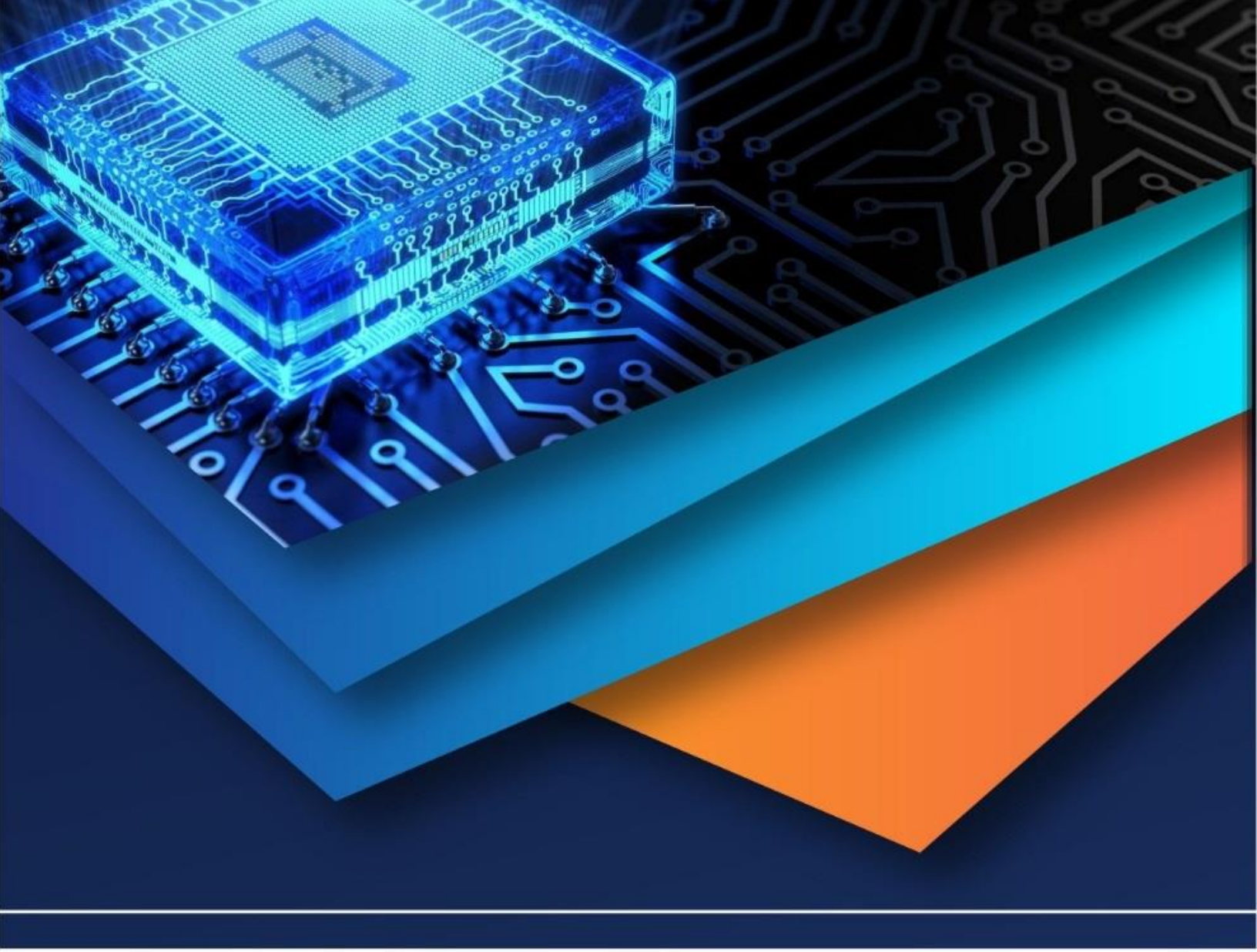
Firstly, we are grateful to Sreenidhi Institute of Science and Technology for giving us the opportunity to work on this project.

We are fortunate to have worked under the supervision of our guide Dr. J. Chattopadhyay. His guidance and ideas have made this project work. We are thankful to Mr. T. Venkat Rao for being the in charge for this project and conduction reviews.

We are also thankful to the HoD of Electronics and Communication Engineering, Dr. S.P.V. Subba Rao for giving us access to all the resources that went into building this project.

REFERENCES

[1] Nisarga, B. and Eric Peeters. “System-Level Tamper Protection Using MSP MCUs.” (2016).
[2] Security Engineering: A Guide to Building Dependable Distributed Systems by Ross J. Anderson, Chapter 14 (Physical Tamper Resistance)
[3] https://people.cs.uchicago.edu/~dinoj/smartcard/securi ty.html#Software%20Security
[4] https://fieldtrack.io/what-electric-door-locks-work/
[5] https://www.atmmarketplace.com/articles/atm- security-part-2-intelligent-locking-systems-and-brute- force-defense/
[6] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/
[7] https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY