IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Tamper Detection Device

[1]Sai Sreekar K S , [2]S Sathya Prakash, [3]M Sai Harshith, [4]Dr. S. Ramani*

Associate Professor,

Department of Electronics and Communication, SNIST, Hyderabad-501301, India,

[1,2,3]B.Tech Scholars, Department of ECE, SNIST, Hyderabad-501301, India.

ABSTRACT:

Tamper Proof Device is used to detect any sort of movement or disturbance. This device gives alert when someone interferes with the system in order to cause damage or make unauthorised alterations. This device consists of MPU6050 which is a Micro Electro- mechanical system (MEMS), it consists of three-axis accelerometer and three-axis gyroscope. It helps us to measure velocity, orientation, acceleration, displacement and other motion like features. The security device further includes Radio Frequency Identification (RFID) circuit configured to provide access to the device. The device includes a microcontroller (ESP32D chip), RFID reader and MPU. When there is an unauthorised alteration detected from the device the system activates the interrupt function which will send an alert message to the authorised mobile number and also gives a warning alarm. This system is enabled with deep sleep mode for maximum power savings. Further this can be used to protect embedded system and in military applications. A tamper detection device can determine whether a housing containing a device has been tampered with either by having the housing penetrated or by an attempt to remove a cover from the housing. The tamper detection device may be a capacitor which is placed across a portion of the housing and whose capacitance changes if it is penetrated. The temper detection device may also be a flexible circuit having conductive strips thereon forming a circuit with means to cause an open circuit if the housing is penetrated or the cover removed from the housing.

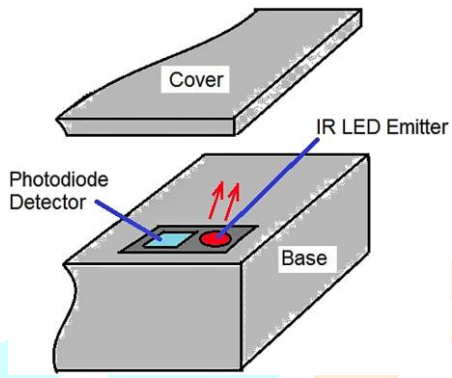
Keywords — ESP-32 Chip, RFID, MPU6050, MEMS.

I.INTRODUCTION

Tamper Proof Device is used to detect any sort of movement or disturbance. This device gives alert when someone interferes with the system in order to cause damage or make unauthorized alterations. Whenever there will be any sort of disturbance caused to the device then automatically the device gets triggered and there will be an alert message that will be sent to our respective Mobile Phones. This technology or this type of device is very useful for the ones who keep their valuables in the device and leave their house. This device runs on a rechargeable battery and apart from that the Chip or the Microcontroller present in this device is enabled with Deep Sleep Mode for Maximum Power Savings. Hence, the device at once can stay active for 3-4 days continuously.[1]

In order to get authorized access an RFID (Radio Frequency Identification) module is used which is integrated inside the device with the Microcontroller. An RFID tag is used is to used to unlock the device and get the access to the device. If a correct RFID tag is placed in front of the RFID module than is present in the device then it is considered to be an Authorized access. A wrong RFID tag leads to an Unauthorized access to the device and gives an alert.[2]

In future this technology can be used by the Personnel to save the Encrypted data or any other Confidential Information. If there will be an Unauthorized access then the whole data will be erased at once. An Authorized access is needed to access to the data.[3]



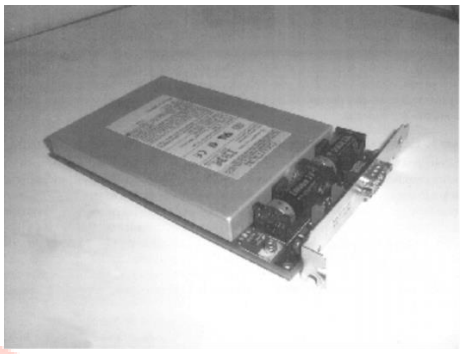


Fig - 1&2: These are the two tamper detection devices

The tamper detection design can be implemented to sense different types, techniques, and sophistication of tampering, depending on the perceived threats and risks.The methods used for tamper detection are typically designed as a suite of sensors each specialized on a single threat type, some of which may be physical penetration, hot or cold temperature extremes, input voltage variations, input frequency variations, x-rays, and gamma rays.[4]

Examples of techniques used to detect tampering may include any or all of the following: switches to detect the opening of doors or access covers, sensors to detect changes in light or pressure.[5]

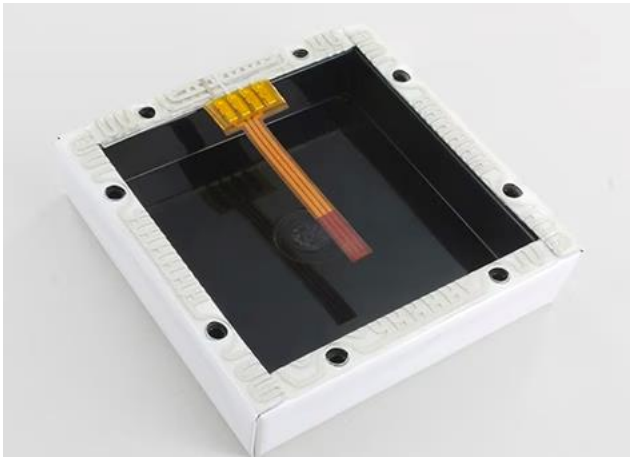


Fig - 3: Basic outline of a Tamper Detection Device

Fig - 4:- Tamper Detection Device

Circuit Diagram and Hardware used

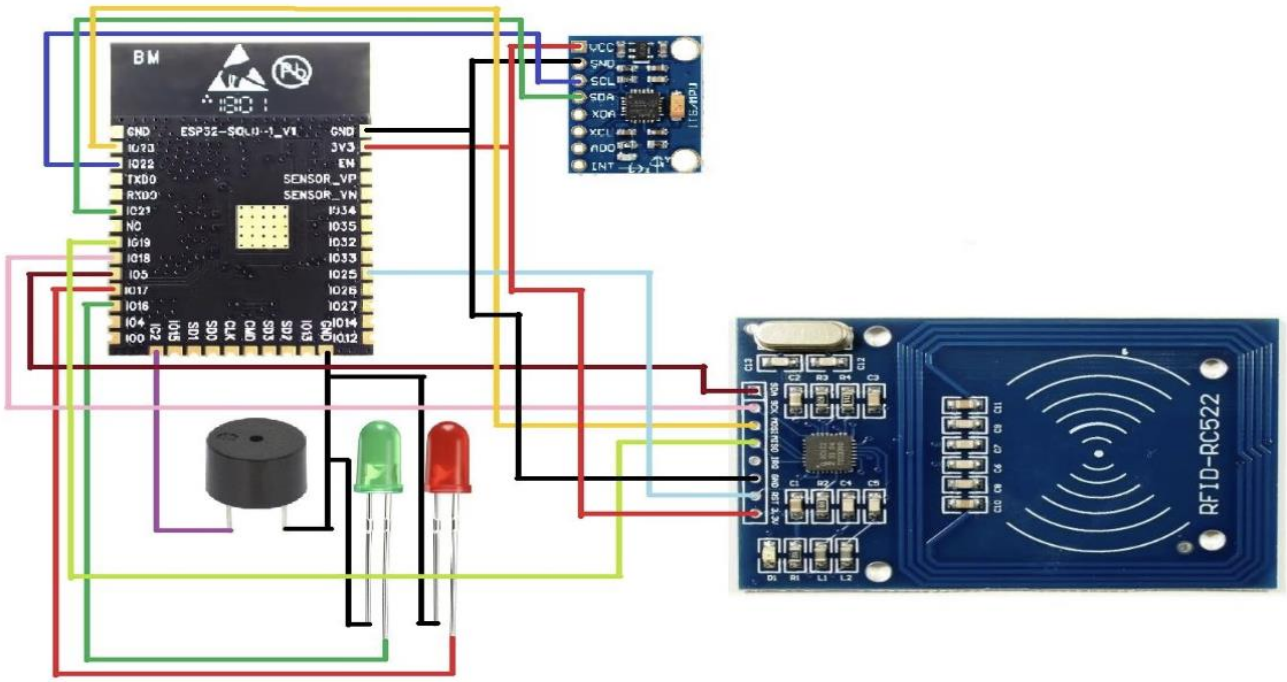


Fig - 5:- Circuit Diagram

This Tamper Detection Device is custom designed both in terms of shape and size as well as the electronics and the hardware are embedded on a custom PCB. This outer casing of this device is totally 3D Printed. The device is easy to install and portable and it has a long battery life, however it is also rechargeable. This Tamper Detection Device is directly connected to the battery. It also has a Comparator chip which helps to measure and digitize the Analog Signals.

The important components used to make this device are ESP32D Chip, MPU6050 and RFID. These components play a key role in the functioning of the Tamper Detection Device, which makes it very easy to use.

Working of the Device

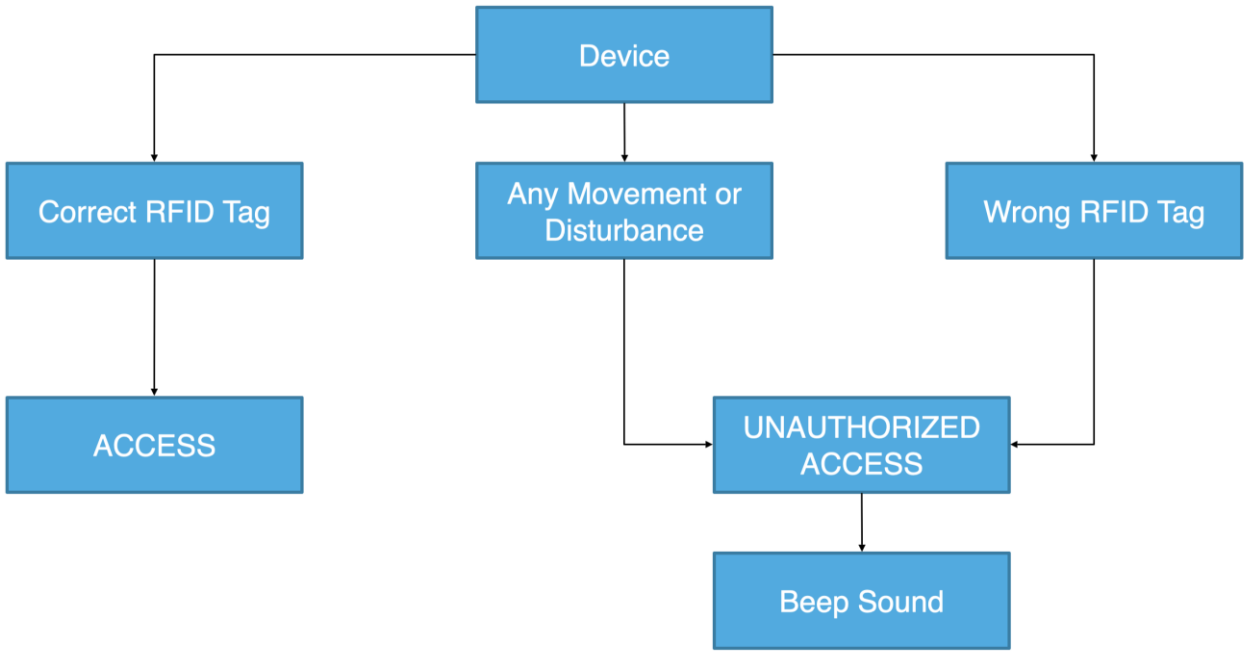


Fig - 6:- Flow Chart to explain the working of the Device

- After the assembling of the device now this is used to detect any sort of movement and disturbance.
- If a disturbance occurs to this device the MPU6050 detects it and directly sends this information to the ESP32-D Chip(Microcontroller) and buzzer starts beeping indicating that there has been an unauthorized access to the device.
- An RFID module is kept inside the device which can be accessed by a particular RFID tag which has to be initialised in the code before itself.
- If a wrong RFID is tag is used, even then the buzzer starts beeping indicating that there has been an unauthorized access to the device.
- A message or a Notification will be sent to the device directly after the object has been disturbed.

Results

Hence, as mentioned above if there is any sort of movement or any disturbance then the buzzer starts beeping automatically and an automated message or a notification will be sent directly to our mobile phones.

This process can be explained in three states which are as follows:-

1. **Initial state:**

Fig - 7:- Device in Normal State

2. **Active state:**

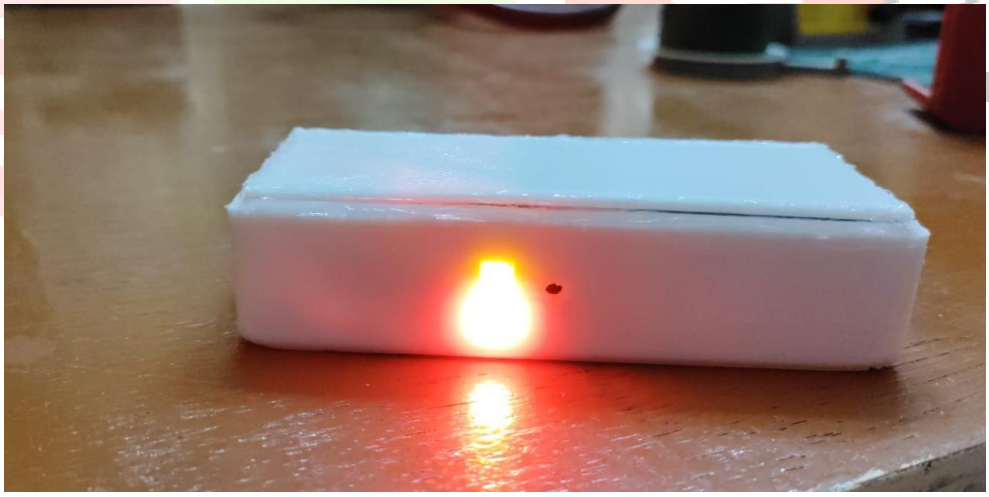


Fig - 8:- LED indicating there has been a movement or disturbance

3. **Receiving Message:**

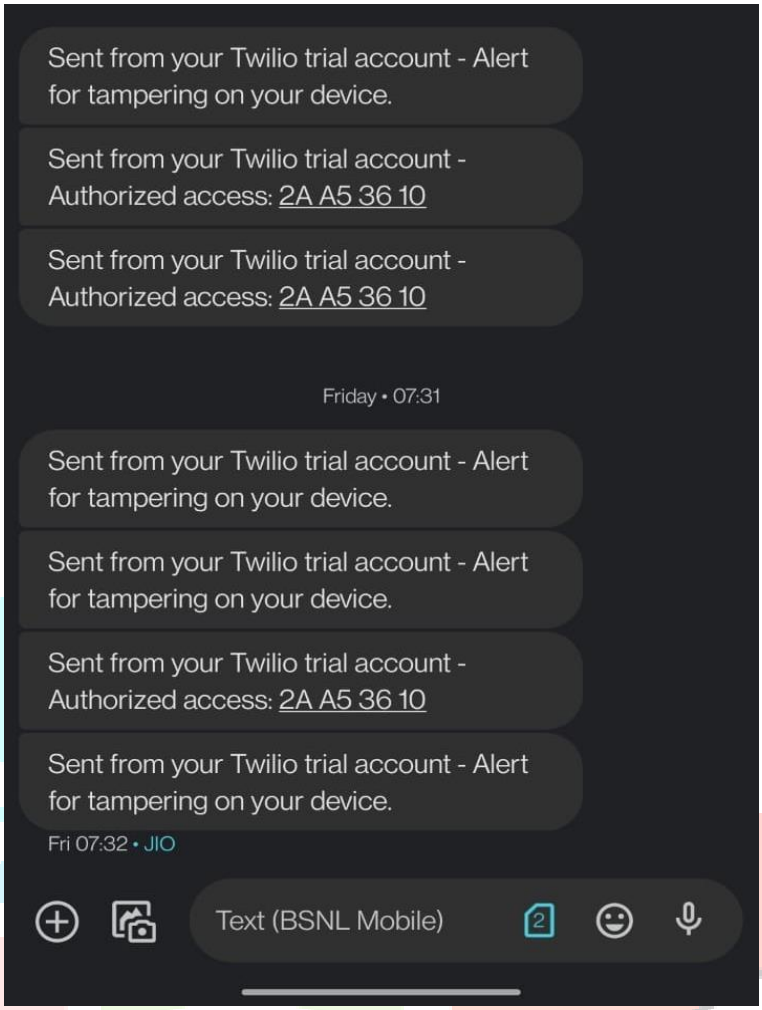


Fig - 9:- Receiving Alert as well as Authorized Access Message

Applications:

- Small things can be easily stored and secured.
- Used to store Encrypted data.
- Small and Portable Design.

Conclusion:

This device mainly focuses to keep our encrypted data safe which is usually stored in the Microcontroller. As soon as there has been an Unauthorized access the whole data is erased. In future this can be very useful for storing the Confidential Information which can be only accessed by the Military Personnel and many others who wants to keep their data encrypted and safe.

References:

- Altera. "Anti-Tamper Capabilities in FPGA Designs". p. 1.
- Johnston, R G (1997). "Physical Security and Tamper-Indicating Devices". LA-UR-96-3827. Vulnerability Assessment Team, Los Alamos National Laboratory. Retrieved 30 August 2019.
- Rosette, J L (2009), "Tamper-Evident Packaging", in Yam, K L (ed.), Encyclopaedia of Packaging Technology, Wiley (published 2010), ISBN 978-0-470-08704-6
- E Biham, A Shamir, "A New Cryptanalytic Attack on DES", preprint, 18/10/96
- E Biham, A Shamir, "Differential Fault Analysis: Identifying the Structure of Unknown Ciphers Sealed in Tamper-Proof Devices", preprint, 10/11/96
- E Biham, A Shamir, "Differential Fault Analysis: A New Cryptanalytic Attack on Secret Key Cryptosystems", preprint, 21/11/96
- M Blaze, personal communication
- M Blaze, "Protocol Failure in the Escrowed Encryption Standard", in Proceedings of the 2nd ACM Conference on Computer and Communications Security (2–4 November 1994), ACM Press, pp 59–67
- F Bao, RH Deng, Y Han, A Jeng, AD Nirasimhalu, T Ngair, "Breaking Public Key Cryptosystems in the Presence of Transient Faults", this volume
- D Boneh, RA DeMillo, RJ Lipton, "On the Importance of Checking Computations", preprint, 11/96
- E Bovenlander, invited talk on smartcard security, Eurocrypt 97
- P Farrell, personal communication
- L Guillou, comment from the floor of Crypto 96
- P Gutman, "Secure Deletion of Data from Magnetic and Solid-State Memory", in Sixth USENIX Security Symposium Proceedings (July 1996) pp 77–89
- M Joye, F Koeune, JJ Quisquater, "Further results on Chinese remaindering", Universit´e Catholique de Louvain Technical Report CG-1997-1, available at
- O Kocar, "Hardwaresicherheit von Mikrochips in Chipkarten", in Datenschutz und Datensicherheit v 20 no 7 (July 96) pp 421–424
- C Mitchell, S Murphy, F Piper, P Wild, "Red Pike — An Assessment", Codes and Ciphers Ltd 2/10/96
- RL Rivest, "The RC5 Encryption Algorithm", in Proceedings of the Second International Workshop on Fast Software Encryption (December 1994), Springer LNCS v 1008 pp 86–96
- 'VISA Security Module Operations Manual', VISA, 1986