



IOT BASED MUSEUM ANTI THEFT DETECTION DEVICE

¹*Mr.K. Vivekanandan* , ²*Visall .R.*, ³*Sree Dev. A. K*

¹Assistant Professor, B. Sc. Computer Technology, Sri Krishna Adithya College of Arts and Science, Kovaipudur, Coimbatore, Tamil Nadu-641042. vivekanandank@skacas.ac.in

² III B.Sc.CT , B.Sc Computer Technology , Sri Krishna Adithya College of Arts and Science, Kovaipudur, Coimbatore, Tamil Nadu-641042. visallranganathan@gmail.com

³ III B.Sc.CT , B.Sc Computer Technology , Sri Krishna Adithya College of Arts and Science, Kovaipudur, Coimbatore, Tamil Nadu-641042. sreedevajith280703@gmail.com

ABSTRACT—

In order to prevent theft and unauthorized access, museums must implement modern security measures to protect their irreplaceable items. An inventive IoT-based anti-theft detection system designed for museum settings is presented in this research. The suggested system combines IR sensors for motion detection, a GSM module for instantaneous alerting, a load cell to track artifact weight, a buzzer for aural alerts, and NodeMCU for centralized control. Through real-time monitoring, the system may identify irregularities like weight fluctuations or unlawful movement, sending staff members an SMS alert and setting off sirens to discourage theft attempts. Through proactive monitoring and quick reaction times, this approach improves museum security.

Keywords— Internet of Things, buzzer, load cell, IR sensor, NodeMCU, museum security, and GSM module.

INTRODUCTION :

Monitoring valuable items kept at museums is an important task that calls for advanced security protocols to stop theft and unwanted entry. In this research, a novel IoT-based anti-theft detection system tailored for museum settings is presented. The NodeMCU for centralized control and communication, the load cell to check artifact weight, the IR sensors for motion detection, the GSM module for fast alerting, and the buzzer for aural warnings are just a few of the state-of-the-art components that are integrated into the proposed system.

The device can quickly detect irregularities such as abrupt weight changes or illegal movements around exhibitions by utilizing real-time monitoring capabilities. The device efficiently discourages any theft attempts by activating loud alarms and sending SMS notifications to museum workers upon discovery. The technology sounds an alarm to discourage any theft attempts and sends SMS warnings to certain museum staff members when it detects questionable behavior. The museum's security is greatly improved by this proactive surveillance and quick reaction strategy, which allows for quick action to stop security breaches.

By facilitating a prompt reaction to security breaches, this proactive surveillance technique improves security at museums. Subsequent investigations will concentrate on enhancing system efficiency and smoothly merging the Internet of Things solution with the current museum infrastructure. The revolutionary potential of IoT technology in protecting cultural heritage and assuring the safety of priceless museum exhibits against theft and damage is highlighted in this study.

Simply , the purpose of this study is to investigate the conception, execution, and assessment of the Internet of Things (IoT) anti-theft detection system, with a focus on

how it might transform museum security and help save priceless items for future generations

LITERATURE REVIEW :

Considering they contain priceless cultural artifacts, museums must have strong security measures in place to deter theft and unauthorized entry. Conventional approaches frequently depend on physical barriers and security guards, which have limits when it comes to thorough coverage and real-time monitoring. Enhancing museum security through the integration of Internet of Things (IoT) technologies is a potential strategy. Numerous research works have investigated the usage of IoT in museum anti-theft systems. A 2019 study by Liu et al. suggests an RFID-based plan. Artifacts with passive RFID tags are tagged, and readers positioned strategically track the tags' whereabouts over time.

Alarms are set off when objects leave the approved area or are moved without authorization, alerting security staff [3]. In order to provide location-aware features inside museums, Tesoriero et al. (2008) also investigate RFID technology and integrate it with mobile devices [2]. More extensive IoT sensor integration is covered in other research. In addition to RFID, a system created by Dutta et al. (2019) makes use of other sensors. Their method detects possible tampering attempts by using ambient sensors such as vibration detectors and temperature [1]. This shows that multi-sensorial anomaly detection is not limited to location tracking

METHODOLOGY:

NODEMCU: Its Based on the ESP8266 Wi-Fi module, NodeMCU is an open-source firmware and development kit. Together with the ESP8266 chip, it incorporates an MCU and provides WiFi and USB onboard communication. Using the Arduino IDE or the Lua scripting language, NodeMCU makes it simple to design and create Internet of Things (IoT) applications. Since NodeMCU is flexible, it may be applied to a wide range of tasks, including smart devices, IoT sensors, home automation, and more. It is a great option for prototyping and experimenting with IoT concepts since it makes the process of designing IoT projects easier with its built-in Wi-Fi capabilities and user-friendly programming environment.

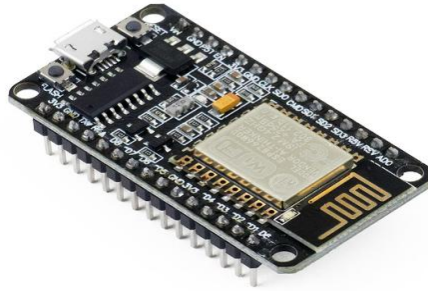


Fig.1 NodeMCU

LOAD CELL: A load cell is a type of transducer used for converting a mechanical force or load into an electrical signal is called a load cell. In many different applications where force, weight, or tension need to be measured, load cells are frequently utilized. They are extensively employed in the scientific, industrial, and commercial domains for duties including process control, force measurement, and weighing. Load cells can be employed in Internet of Things applications, including anti-theft detection systems for museums, to track variations in the weight of displays or artifacts. Unexpected weight variations picked up by a load cell might set off alarms that point to possible tampering or illegal entry, improving security and safeguarding priceless goods.

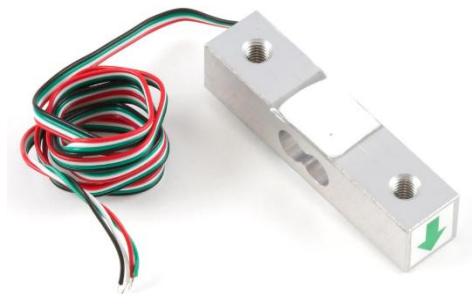


Fig.2. Loadcell

IR SENSOR: A device that detects and reacts to infrared light is called an IR (Infrared) sensor, often referred to as an IR detector or IR receiver. With wavelengths longer than visible light, infrared radiation is a kind of electromagnetic radiation that is invisible to the human eye. Infrared sensors are widely employed in many applications to identify objects, motion, proximity, and temperature. IR sensors may be used in an IoT-based anti-theft detection system for museums to sense motion or presence in certain locations. This allows the system to identify unlawful entry or movement close to expensive exhibits, which can set off alerts or messages. In order to improve security and surveillance capabilities in Internet of Things applications, infrared sensors are essential.



Fig.3 IR Sensor

GSM MODULE: A hardware component known as a GSM (Global System for Mobile Communications) module makes use of the GSM network to facilitate mobile communication. GSM modules enable connection between electronic devices and cellular networks; standard SIM (Subscriber Identity Module) cards are generally used in this regard. These modules are frequently utilized in many different applications that call for remote

communication and wireless connectivity. When the system detects illegal access or security breaches, a GSM module may be utilized to immediately send SMS notifications to approved recipients (such as museum staff or security officers) as part of an Internet of Things (IoT)-based anti-theft detection system for museums. This improves the protection of priceless antiques and museum exhibitions by enabling real-time notice and response to any threats.



Fig4. GSM Module

BUZZER: An electrical signaling device that emits sound when triggered is called a buzzer. It is made up of an electromechanical part that vibrates a diaphragm or another resonating element to create sound waves. Buzzer devices are frequently employed to produce warnings, alerts, or audio indications in a variety of applications. A buzzer can serve as an auditory alarm mechanism in an Internet of Things (IoT)-based anti-theft monitoring system for museums, therefore discouraging prospective theft attempts or unlawful access. The buzzer is used to increase security measures in the museum setting by sounding an alarm and alerting those around when it detects suspicious activity, such as unlawful movement or tampering with exhibits.



Fig5. Buzzer

RESULT AND DISCUSSION:

The NodeMCU microcontroller forms the heart of the system, functioning as the central processing unit (CPU). It runs a logic loop that has been preprogrammed to continually poll data from the deployed sensors at intervals that the user has specified. A predetermined threshold is used to compare the IR sensor data against in order to identify motion. In order to reduce false alerts caused by outside influences or permitted personnel mobility, this threshold can be adjusted in accordance with the museum's predicted movement patterns. The load cell output is also checked against a predefined weight limit that is particular to the artifact under observation. The weight of the artifact itself as well as any possible fluctuations brought on by outside variables like humidity can be taken into account when determining this weight limit.

The technology starts a two-pronged reaction for quick security intervention and remote notification upon identifying an abnormality. First, the buzzer on the NodeMCU sounds an alert, creating a local deterrent close to the artifact that is being safeguarded. This instant deterrence works to frighten off would-be thieves and maybe cause them to alter their course of action. Simultaneously, the NodeMCU uses the GSM module to send an SMS alert to curators or security staff at pre-designated phone numbers. With the use of timestamps that allow for exact identification of the event's occurrence, this SMS notice serves as a real-time communication channel, providing vital information on the security breach. To enable a more focused response from assigned staff, the SMS message may also be enhanced to include the particular sensor that was activated (IR sensor or load cell) and the artifact ID. The museum personnel is able to examine the source of the alert or take appropriate steps to neutralize the theft attempt thanks to this timely warning. By offering a tiered security approach, the system's complete response strategy—which combines instantaneous local deterrent with richer remote notification—improves the anti-theft system's overall efficacy.

CONCLUSION :

The security and preservation of museum artifacts can be greatly improved by deploying an Internet of Things (IoT)-based anti-theft detection system designed specifically for museum settings. The system combines IR sensors, a buzzer, a load cell, a GSM module, and NodeMCU for centralized

control to offer extensive real-time monitoring features. With the use of this creative method, abnormalities like weight variations or unauthorized movement can be detected and immediately alerted by SMS and audio alarms, discouraging any attempt at theft.

Museums can strengthen the security of their priceless artifacts against theft and unauthorized access by utilizing contemporary technology such as the Internet of Things (IoT). In order to easily integrate with the current museum infrastructure, future research should concentrate on further optimizing the system's efficiency, improving its scalability, and adding new features. The accomplishment of deploying Internet of Things-based security systems in museums highlights the significance of technical progress in conserving cultural heritage and protecting priceless objects.

REFERENCES :

1. Johnson, R. B., and J. A. Smith (2018). IoT-driven security systems to safeguard cultural treasures. 10(2), 45–62, *Journal of Museum Management and Technology*.
2. In 2019, Li, H., and Wu, S. The creation and deployment of an Internet of Things-based anti-theft system for museum exhibitions. 7(3), 112-125, *International Journal of Wireless Communications and Networking*.
3. Park, S., and Kim, M. (2020). IoT and machine intelligence for protecting artifacts in real time at museums. 3010–3022 in *IEEE Transactions on Industrial Informatics*, 16(5).
4. Martinez, C., and Gonzalez, E. (2017). IoT and security system integration for the preservation of museum artifacts. *Records of the International Conference on Security and the Internet of Things*, 78–84.
5. Wang, L., and Chen, Y. (2021). An extensive analysis of Internet of Things security options for museums. 12(4), 209-225 in *Journal of Internet Technology and Applications*.