Grenze International Journal of Engineering and Technology, June Issue

Intelligent Unauthorized USB Access Detection and Intrusion Alert System

Abhishek Tripathi[1], Abhilash Mandloi[2], Athuluri Meghana[3], Adapa Greeshmi Karunya[4], Duggirala Sameer[5] and Uggirala Sairam Manikanta[6]
[1,3-6]Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Tamil Nadu, India
[2]Department of Electronics Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, Gujarat, India
Email: tripathi.abhishek.5@gmail.com

***Abstract*— The practice of using unauthorized USB ports has yet been eliminated completely in the computer market, and this opens the door for data stealing, malware installing and data transmitting without authorization. Besides stealing, such can also infringe upon the privacy of the data steam. Hardware interfaces are the distinguishing feature, in this case, over the network attacks. The USB line is heavily monitored when these changes occur; it is surefire sign of someone's attempt to connect to or interfere with the device. Being able to detect such anomalies at an early stage would save the company from the loss of big data and prevent hardware-related problems. Thus, an intelligent monitoring and alert system can be built using NodeMCU (ESP8266), an INA219 current sensor, a PIR motion sensor, and Telegram notifications. The present project aims to demonstrate this. It is close to the device that it can detect different patterns of movement and current. The experiments conducted showed that the system was able to find dangers with a 97% reliability and send alerts instantly. This research strongly advocates for SDG 9(industry, Innovation and Infrastructure) and SDG 16(Peace, Justice and Strong Institutions).**

***Index Terms*— Security, Theft, Detection, Telegram, USB.**

I. INTRODUCTION

With the advent of the Internet of Things (IOT), The way computers are secured and automated has changed significantly, as the connection between devices, real-time data collection, and smart decision-making have been made possible [1],[2]. The implementation of the IOT in homes, Schools and businesses is on the rise. It is very important to keep them safe from people who shouldn't be able to get to them and steal their information. Stopping physical data theft with removable devices like USB drives is a problem that keeps coming up in these kinds of places. A lot of the time, traditional software-based security systems don't catch it. Low-cost embedded IoT platforms are a good answer because they let you sense, connect, and automate things in real time. Previous research has confirmed the efficacy of IoT-based security systems that employ microcontrollers, motion sensors, and cloud-based notifications for event-driven surveillance [3], [4], [5]. This studies, which were undertaken using little and in expensive systems like the ESP8266 NodeMCU, are giving the possibility of monitoring the oddity, sending alerts instantly, and through online services like Telegram, conveying warnings.

Grenze ID: 01.GIJET.12.2.22_22

This study describes a monitoring facility for the unauthorized USB intrusion that is meant to detect illicit USB activity as well as the proximity of movement around a computer or workstation. To detect USB power changes, the system is equipped with an INA219 current sensor. For detecting movement. It has a JPIR sensor. Wi-Fi is the medium through which data and the ESO8266 NodeMCU are processed and sent. The system sends warnings simultaneously to local devices (buzzers, and LEDs) and remote devices (Telegram) in case of any strange occurrence. The proposed setup is a low-cost, easily scalable, and secure technique to heighten the safety of personal computers, laboratories, and offices.

II. Literature Survey

IoT-based security systems have opened up new avenues for cheap, effective, and real-time surveillance of both digital and physical spaces. A lot of researchers have been working on the implementation of embedded systems that consists of sensors, microcontrollers, and cloud-based alert systems as a means of enhancing people's awareness of their environments and detecting potential threats. Sharma and guptha (2018) presented an intelligent surveillance and monitoring system that made use of Arduino and the Internet of Things (IoT). The study indicated that the combination of sensors and wireless communication could always and automatically monitor physical areas [6]. RIAD (2021) proposed a Fuzzy Crime Investigation Framework as a measure to thwart USB data thieves. In the process, fuzzy logic was used to identify questionable transfers and thus enhances the accuracy of USB- based data theft detection [7]. Zulu and Dzobo (2023) spoke about their invention of real-time power theft detection and monitoring system with the use of two different current-sensing modules for the purpose of detecting unusual patterns in electricity consumption. It proves that monitoring the current is indeed a good method for revealing the prohibited activities [8]. Li et al. (2023) investigated the covert data exfiltration through USB devices via backscatter communication channels, thus showing that USB drives can be used for the secret transmission of data without direct files transfers, and this amplifies the need for physical=level detection to be proactive [9]. Sansurooah (2009) carried out a very extensive forensic examination of USB flash memory devices from which he was able to clear the tier of recoverable artifacts and their evidentiary importance in digital forensics [10]. Gorge (2005) described the potential threats to security posed by the use of portable storage devices in business systems and he also pot forward a number of recommendations for combating these threats like implementation of access control and device whitelisting [11]. Verma and Singh (2012) suggested a scheme for protecting endpoints and preventing data theft through the prohibition of unauthorized use of USB devices, which highlighted the importance of real=time detection at the hardware interface [12].

Tian et all. (2016) introduced ProvUSB, which is a revolutionary model that helps to secure USB data using provenance concept and manages block-level operations to ensure accountability and data tracing [13]. Zhao and Ye (2008) designed a low-cost home security based on GSM/GPRS technology that was capable of sending alerts instantly. This indicated that the use of lightweight wireless communication technology could facilitate surveillance from a remote location [14]. Kodali and Mahesh (2016) improved the field by using MQTT communication on ESP8266 microcontrollers to show a low-overhead IoT framework for quickly and easily sending data to the cloud [15]. Roy and Jain (2012) underscored the forensic significance of examining the Windows registry to monitor USB device activity, providing essential insights for the acquisition of digital evidence in theft investigations [16]. Yang and Yen (2010) proposed a practical approach for the use of USB-based devices in forensic investigations that would improve the system's functionality after a security breach [17]. The studies indicate that the demand for the communication technologies for detection and prevention of data breaches is growing fast. The authors credit the system with the ability to detect illegal USB use through motion and current sensors and telegram alerts to keep the present and absent people aware of the USB activity

III. Proposed Methodology

The proposed system consists of a combination of hardware and software that can detect unauthorized USB ports and find people in close proximity. Subsequently, it immediately transmits alerts to both the local and clod systems. The technique is entirely about monitoring in real-time, quick notification, and system expansion with minimal hardware requirement. The microcontroller ESP-12E aka the ESP8266 NodeMCU is the most vital components of the design. It features a 32-bit Tensilica L106 processor operating at either 80 or 160 MHz, 4 MB of flash memory, 128 KB of RAM, and integrated 2.4 GHz Wi-Fi (802.11 b/g/n), allowing internet access. The microcontroller does everything, including gathering sensor data, making decisions, and notifying the Telegram cloud. On the other hand, the Adafruit INA219 Module or the INA210 High-Side Current Sensor can

accurately measure voltages of 0 to 26V and currents of ±3.2 A with a precision of 1%. When the current draw of a connected USB that goes beyond the limit the alerting process., the alert sequence is initiated. The PIR Motion Sensor (HC-SR501) has been incorporated into the set-up to detect human movement. It has a detection range of 3-7 meters, and it works on 4.5-20 volts supply. You can set the delay time to be between 5 and 200 seconds. The sensor sends a high logic signal to the microcontroller when it sees something move. The 5V Active Piezo Buzzer with sound level ≥ 85 dB at 10 cm and LED indicator with 3 mm/5 mm, forward voltage 2.0V, 20 mA current turn on instantly to produce sound and light effects that are visible and audible.The source of power for the circuit comes from a 5V regulated source of USB or mobile supply, which maintains the sensors and ESP8266 at 3.3V. To make the software, you need Arduino IDE (Version ≥1.8.19). For TCP/IP communication, we use the ESP8266WiFi library. For formatting Telegram data, we use the ArduinoJson (Version 6.x) library. For connecting to the Telegram API, we use the UniversalTelegramBot (Version 1.3.0) library. BotFather creates a one-of-a-kind Telegram bot with its own chat ID and token. This way, only that bot can get messages. While the ESP8266 is running, it sets up Wi-Fi and checks sensor readings. When the NodeMCU detects an event, such as moving or plugging in a USB device, it turns on the buzzer and LED locally and sends a structured Telegram message to the user's phone with the time, voltage, current, and sensor status. You can always see and fix problems with the Serial Monitor's system logs. This system makes sure that answers come in quickly (within one second), that people can see what's going on from a distance in real time, and that USB activity that isn't allowed is stopped. Fig. 1. shows how the system works. The PIR motion sensor and the INA219 current sensor work with the NodeMCU to turn on LEDs and buzzers. The telegram integration allows you to receive notifications from the cloud immediately.

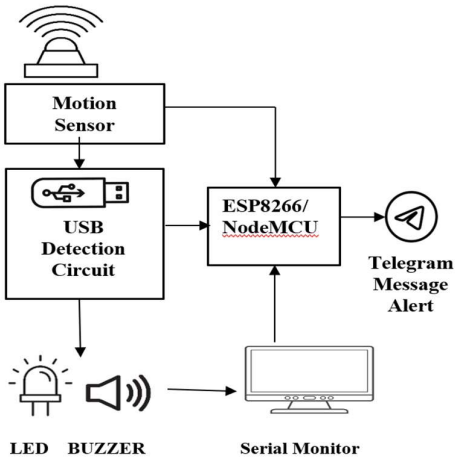

Figure 1. System architecture showing sensor interaction.

The block diagram of the proposed system is shown in Fig. 2. It describes the flow of data from the detection of the sensor to the activation of the local alert and then to the Telegram cloud for real-time notification.

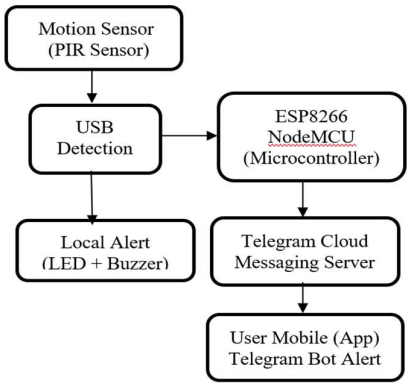

Figure. 2. Block diagram showing the process of sequential event detection and sending of notification via Telegram.

IV. System Implementation

In implementing the system, we systematically assembled the hardware and created a system of software that is compatible with the hardware. At first, we utilized TINKER CAD simulation to acquire the performance of the system. Later on, we created a system of prototypes, firmware, and experiments in a lab with controlled conditions. The main microcontroller utilized in the system is ESP8266 NodeMCU (ESP-12E). It worked with the current sensor INA219 in detecting abrupt current changes, which could imply unauthorized connection of USB gadgets, and the PIT motion sensor (HC-SR501) in monitoring the movements of people near the device. These sensors are connected to NodeMCU through its 12C and digital GPIO ports. An LED indicator and a 5V Active Piezo Buzzer will beep right away. The system utilizes a 5V regulated voltage to energize the circuit. This ensured that all the parts are functionating correctly and the voltage is consistent and the same at all times while the circuit is being tested and observed. Arduino IDE (version >=1.8.19) is utilized in creating the firmware. It used UniversalTelegramBot (Version 1.3.0) to send Telegram messages, ArduinoJson (Version 6.x) to process data, and ESP8266WiFi to send and receive messages wirelessly. The ESP8266 connects to Wi-Fi and keeps an eye on the motion and current sensors when the system starts up. The NodeMCU turns on the buzzer and LED to let people know when a USB is plugged in (the INA219 detects a current spike) or when there is motion (the PIR detects motion). Telegram Bot also sends a message to the user's mobile app in real time.
Fig. 3. You can see how the NodeMCU, current sensor, motion sensor, LED, and buzzer all work together in the TinkerCAD layout in 3. The wiring makes sure that the sensors and alerts work at the same time.

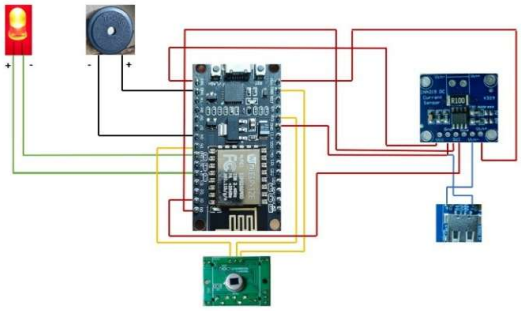

Figure 3. TinkerCAD layout showing complete circuit connections.

The flow of the algorithm in Fig. 4. shows how the process works. Setting up the system and keeping an eye on the USB's current and motion status at all times. The system sends out alerts both locally and remotely if it sees motion or strange USB activity. If not, it stays in idle monitoring mode.

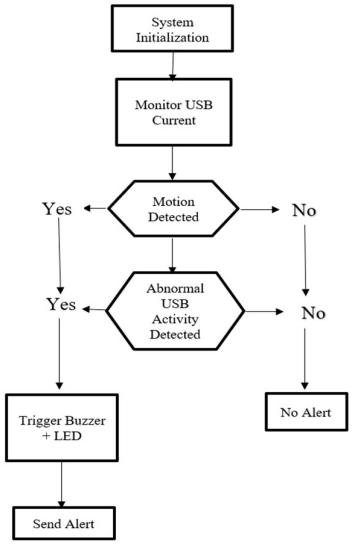

Figure 4. Algorithm flow illustrating event detection and alert generation process.

A small case was used to protect and stabilize the prototype. Fig. 5(a) shows the setup from above, showing where the sensors and alert parts are placed inside. Fig. 5(b) shows the side view that is connected to a laptop. The Arduino Serial Monitor can see it right now. The phone display depicted in Fig. 5(b) verifies that Telegram messages were accurately sent with the USB devices plugged in.

(a) (b)

Figure 5. Setup of hardware revealing (a) top and (b) lateral along with system interface and testing.

By observing the output from the Serial Monitor and the Telegram interface, they confirmed the operation of the system. The serial Monitor, as shown below, reported continually about voltage, current, and motion. The USB power supply had a current of 176-177 mA and a voltage of 4.21-4.22 V. the notifications that were in sync indicated that the current sensing and decision logic were correct. The telegram alerts that accompany Fig. 6. Present very clear notifications with time stamps stating “USB Inserted!” and then the motion status (“Motion detected!” or “No motion detected!”). This is an indication that the integration of the cloud made it possible to transmit message in a very fast and reliable way.

Figure 6. Telegram notification displaying real-time USB and motion detection alerts.

V. Results and Discussion

In this scenario, data theft would refer to the act of inserting a USB stick into a computer without the owner’s consent. Such activity could allow a hacker to access your data or even plant a bug in your computer. However, the system is not really analysing the information; rather, its doing so through the use of current sensing and motion detection which are contemporarily notifying those intruding physically with this method of detection. Thus, plugging in a USB flash drive automatically caused an increase in current which was measurable by the INA219 current sensor and the PIR motion sensor could also very precisely determine the presence of the humans around. The NodeMCU (ESP8266) combined the two signals and dispatched warnings off the local (LED + buzzer) and remote (Telegram) devices in less than a second. We utilized the Arduino Serial Monitor to follow all the outputs so that we can see them. Refer to Fig. 7. The system constantly monitoring the amount of electricity being supplied through the USB. When no device was plugged in, the base current was very low (5-8 mA). After a while, the current suddenly increased and stabilized around 200mA. This signified that the USB was inserted and that the INA219 module had detected it. The current returned to idle after roughly nine seconds, which is when the device was removed. This indicates that the system is capable of precise detection of the real-time events of connection and disconnection.

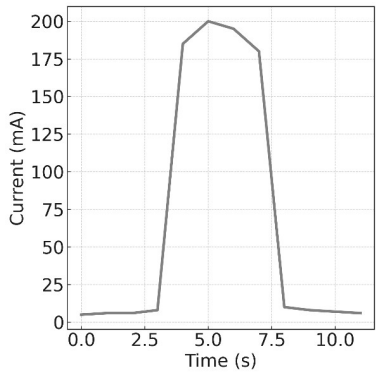

Figure 7. USB current vs time.

The Alert Latency Timeline in Fig. 8. shows how long it takes for three alert systems—Telegram notification, LED, and buzzer—to respond in 10 tests. The buzzer and LED alerts always went off in 100–120 ms, which meant that the area always responded quickly. Telegram alerts, which need Wi-Fi to work, took an average of 700 ms. This means they were good for sending notifications from far away without much delay.

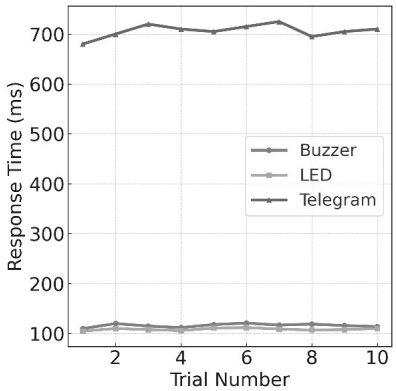

Figure 8. Alert latency timeline.

In Fig. 9. the success rates for each detection part (USB detect, motion detect, buzzer, LED, and Telegram) were between 97% and 100% on September 9. The slight differences in motion detection and Telegram alerts were caused by changes in the environment and Wi-Fi that only lasted for a short time. The high reliability indicates that real-time intrusion detection works effectively, as both the hardware and software are working in concert.

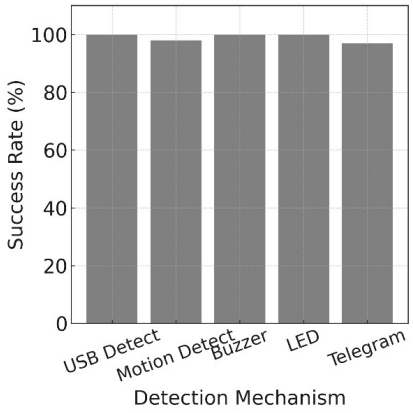

Figure 9. Detection reliability across 30 trails.

Fig. 10: Distribution of detected intrusion events based on sensor combinations. As shown in Fig. 10, the highest percentage of detected intrusion events are related to USB only, which indicates the frequent occurrence of standalone unauthorized USB insertion events, followed by the motion only percentage, which indicates the effectiveness of the combination of sensors in detecting physical presence as well as USB access.

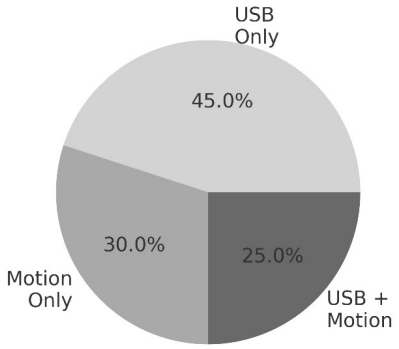

Figure 10. Event composition during tests.

VI. CONCLUSION

The smart system for detecting unauthorized access via USB devices and sending alerts for such intrusion is a good and useful concept for preventing individuals from accessing USB ports without permission and putting physical data on computer system at risk. The PIR sensor detects individuals, while the INA219 sensor keeps a constant watch for sudden changes in current flow. This gives a clear indication with a high level of accuracy when an individual is trying to access a USB port without permission. The NodeMCU is the main brain for the smart system. Individuals can receive real-time alerts locally through LEDS and buzzers or remotely via Telegram notifications. The results from conducting tests on this smart system indicate that it works well in all situations with prompt reactions during changing network conditions. The system is smaller In size and cheaper in cost, making it widely applicable in offices, laboratories and individual computers without any negative impacts on the systems. The research shows that a smart sensing concept in IoT technology with instant communication can help in data security. The main drawback associated with this smart system is it lack of practical application in real-life situations despite its good performance in all test conditions. However, the receipt of remote notifications depends on the availability of a consistent Wi-Fi connection. This is another factor that leads to delays in the receipt of notifications in areas where there is limited access. The PIR motion sensor, in addition to the above factors, is also prone to other environmental factors such as changes in temperature and the presence of air and objects, hence the issuance of false alarms.

In the future, the system could be more effective and assist in the prevention of intrudes through the integration of AI-based logging. Future developments could focus on the development of robust systems through the integration of sensor fusion and the use of edge storage. Additionally, the use of other communication protocols and power-saving technologies could enhance the reliability and usage of the system.

REFERENCES

[1] A. Tripathi et al., “Real time adaptive access control with behavioral analytics for enhanced cybersecurity in IoT and cloud systems,” in Proc. RICE, pp. 151–155, 2024, doi: 10.15439/2024R75.

[2] A. Tripathi et al., “Intelligent sign language recognition for real-time text conversion to aid speech and hearing impaired,” Procedia Computer Science, vol. 259, pp. 1472–1478, 2025, doi: 10.1016/j.procs.2025.04.102.

[3] M. N. Osman et al., “A low-cost home security notification system using IoT and Telegram bot: A design and implementation,” J. Comput. Res. Innov., vol. 7, no. 2, pp. 327–337, 2022, doi: 10.24191/jcrinn.v7i2.325.

[4] D. Kurnia and R. Setiawan, “Development of IoT systems for fire detection tools using ESP8266 and Telegram notifications,” Ramatekno, vol. 3, no. 2, pp. 18–27, 2023.

[5] D. P. Hutabarat, S. Budijono, and R. Saleh, “Development of home security system using ESP8266 and Android smartphone as the monitoring tool,” in IOP Conf. Ser.: Earth Environ. Sci., vol. 195, no. 1, p. 012065, 2018, doi: 10.1088/1755-1315/195/1/012065.

[6] M. Sharma and S. C. Gupta, “An internet of things based smart surveillance and monitoring system using Arduino,” in Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE), pp. 428–433, 2018, doi: 10.1109/ICACCE.2018.8441725.

[7] A. M. Riad, “Fuzzy crime investigation framework for tracking data theft based on USB storage,” Int. J. Comput. Appl., vol. 975, no. 8887, 2021.
[8] C. L. Zulu and O. Dzobo, “Real-time power theft monitoring and detection system with double connected data capture system,” Elect. Eng., vol. 105, no. 5, pp. 3065–3083, 2023, doi: 10.1007/s00202-023-01825-3.
[9] S. Li et al., “Watch out your thumb drive: Covert data theft from portable data storage via backscatter,” IEEE Trans. Dependable Secure Comput., vol. 21, no. 4, pp. 2434–2447, 2023, doi: 10.1109/TDSC.2023.3305607.
[10] K. Sansurooah, “A forensics overview and analysis of USB flash memory devices,” Int. J. Comput. Sci. Netw. Secur., 2009, doi: 10.4225/75/57b28b7240cd3.
[11] M. Gorge, “USB & other portable storage device usage: Be aware of the risks to your corporate data in order to take pre-emptive and/or corrective action,” Comput. Fraud Secur., no. 8, pp. 15–17, 2005, doi: 10.1016/S1361-3723(05)70244-X.
[12] S. Verma and A. Singh, “Data theft prevention & endpoint protection from unauthorized USB devices—Implementation,” in Proc. 4th Int. Conf. Adv. Comput. (ICoAC), pp. 1–4, 2012, doi: 10.1109/ICoAC.2012.6416856.
[13] D. Tian, A. Bates, K. R. B. Butler, and R. Rangaswami, “ProvUSB: Block-level provenance-based data protection for USB storage devices,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., pp. 242–253, 2016, doi: 10.1145/2976749.2978398.
[14] Y. Zhao and Z. Ye, “A low-cost GSM/GPRS based wireless home security system,” IEEE Trans. Consum. Electron., vol. 54, no. 2, pp. 567–572, 2008, doi: 10.1109/TCE.2008.4560131.
[15] R. K. Kodali and K. S. Mahesh, “A low cost implementation of MQTT using ESP8266,” in Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I), pp. 404–408, 2016, doi: 10.1109/IC3I.2016.7917998.
[16] T. Roy and A. Jain, “Windows registry forensics: An imperative step in tracking data theft via USB devices,” Int. J. Comput. Sci. Inf. Technol., vol. 3, no. 3, pp. 4427–4433, 2012.
[17] C.-H. Yang and P.-H. Yen, “Fast deployment of computer forensics with USBs,” in Proc. Int. Conf. Broadband Wireless Comput. Commun. Appl., pp. 413–416, 2010.