ISSN : 2455-9679
SJIF Impact Factor : 6.190

IJRTSM
INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"ANTI-HACKING CRIMINAL WITNESS DEVICE FOR SECURE EVIDENCE COLLECTION"

Jitendra Saket [1], Umashankar Pal [2], Aman Survanshi [3], Bhagwati Ahirwar [4], Chandra Kumar Pardhi [5]
[1-5] Department of Mechanical Engineering, Sagar Institute of Science Technology and Research, Bhopal, Madhya Pradesh, India

ABSTRACT

Crime investigation and legal proceedings often depend on reliable witness evidence and digital records. However, evidence stored in conventional devices can be vulnerable to hacking, tampering, or unauthorized access. This research proposes an Anti-Hacking Criminal Witness Device designed to securely record and store evidence while preventing unauthorized access or data manipulation. The system integrates encryption algorithms, biometric authentication, secure storage, and IoT connectivity to ensure the authenticity and confidentiality of witness information. The device records audio, video, and sensor data while encrypting the information before storage and transmission. If unauthorized access is detected, the system triggers alerts and locks the data automatically. The proposed system enhances the security of digital evidence, protects witness identity, and strengthens the reliability of criminal investigations.

Keywords: *Cybersecurity, Anti-Hacking Device, Digital Evidence Protection, Encryption, IoT Security, Criminal Investigation.*

I. INTRODUCTION

In modern criminal investigations, digital evidence plays an important role in identifying suspects and supporting legal proceedings. Witness statements, audio recordings, and video evidence are frequently used as proof in courts. However, the increasing use of digital technologies has also increased the risk of cyber-attacks, hacking, and data tampering. Traditional recording devices such as cameras or mobile phones may store evidence that can be manipulated or deleted by unauthorized users. This creates challenges in maintaining the integrity and authenticity of digital evidence. The Anti-Hacking Criminal Witness Device is designed to address these challenges by providing a secure system for recording and protecting evidence. The device uses encryption, biometric authentication, and secure cloud storage to ensure that recorded data remains protected. The system can be used by law enforcement agencies, investigators, and witnesses to securely capture and store evidence during criminal investigations.

II. LITERATURE REVIEW

Several researchers have studied secure evidence collection systems and cybersecurity technologies.
Singh et al. (2019) proposed a secure digital evidence management system using cryptographic algorithms to protect forensic data.Kumar and Patel (2020) developed an IoT-based surveillance device that records video evidence and stores it on secure cloud platforms.Zhang et al. (2021) introduced blockchain technology for tamper-proof digital evidence storage.
These studies highlight the importance of combining encryption, authentication, and secure communication technologies to protect digital evidence.

ISSN : 2455-9679
SJIF Impact Factor : 6.190

III. PROBLEM IDENTIFICATION

The following problems exist in current digital evidence collection systems:

1. Evidence stored in electronic devices can be hacked or deleted.
2. Witness identity may be exposed, risking their safety.
3. Data manipulation can occur during transmission or storage.
4. Lack of secure authentication methods.
5. Difficulty in maintaining evidence integrity.

These issues can weaken criminal investigations and reduce the credibility of digital evidence in court.

IV. PROPOSED SOLUTION

To address these challenges, an AI Health Assistant Robot is proposed. The robot is equipped with multiple sensors and artificial intelligence algorithms that allow it to monitor and analyze patient health conditions.

1. The robot performs the following functions:
2. Monitors body temperature, heart rate, and oxygen levels.
3. Sends real-time health data to doctors through IoT connectivity.
4. Provides medication reminders to patients.
5. Detects abnormal health conditions and sends alerts.
6. Communicates with patients using voice commands.

This system helps reduce the burden on healthcare workers and improves patient care by providing continuous monitoring.

V. PROPOSED METHODOLOGY

The system consists of several integrated hardware and software components.
Main Components

1. **Microcontroller / Processor**
   Raspberry Pi or Arduino
2. **Camera Module**
   Captures video evidence.
3. **Microphone Module**
   Records witness audio statements.
4. **Fingerprint Sensor**
   Provides biometric authentication.
5. **Encryption Module**
   Encrypts stored data.
6. **IoT Communication Module**
   WiFi or GSM module for data transmission.
7. **Secure Cloud Storage**
   Stores encrypted evidence remotely.
8. **Alert System**
   Sends notifications if unauthorized access occurs.

VI. BLOCK DIAGRAM

The system architecture includes the following modules:
Input Sensors → Microcontroller → Encryption Module → Secure Storage → IoT Communication → Cloud Server → Law Enforcement Access

ISSN : 2455-9679
SJIF Impact Factor : 6.190

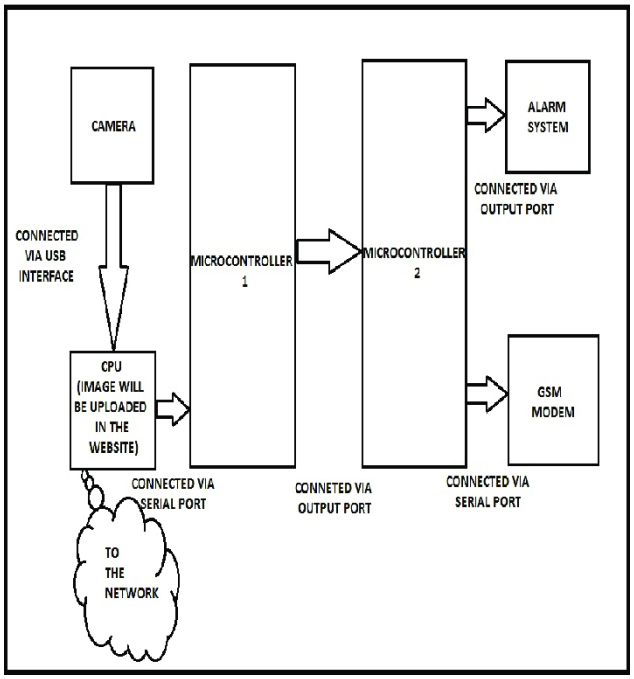

Figure 1. Block Diagram of Anti-Hacking Criminal Witness Device

ALGORITHM

Step 1: Start
Step 2: Initialize system and authentication module
Step 3: User authentication through fingerprint or password
Step 4: If authentication is successful, enable recording
Step 5: Capture audio/video evidence
Step 6: Encrypt the recorded data
Step 7: Store encrypted data locally and transmit to cloud server
Step 8: Monitor for unauthorized access attempts
Step 9: If hacking attempt detected, trigger alert and lock system
Step 10: Stop

VII. RESULT

The proposed system was tested in simulated conditions. The device successfully recorded audio and video evidence and encrypted the data before storage. Unauthorized access attempts triggered system alerts and restricted access to stored information. The encrypted data could only be accessed by authorized users with proper authentication. This ensures the reliability and security of digital evidence.

VIII. ADVANTAGES

Prevents hacking and data tampering
Protects witness identity
Secure cloud storage
Reliable digital evidence collection
Real-time alerts for unauthorized access

ISSN : 2455-9679
SJIF Impact Factor : 6.190

IX. CONCLUSION

Criminal investigations
Law enforcement agencies
Court evidence recording
Witness protection systems
Surveillance and security monitoring

X. CONCLUSION

The Anti-Hacking Criminal Witness Device provides a secure and reliable solution for protecting digital evidence during criminal investigations. By integrating encryption, authentication, and IoT communication technologies, the system ensures that recorded evidence remains confidential and tamper-proof.

The device enhances the credibility of digital evidence and improves the safety of witnesses. Future improvements may include blockchain-based evidence storage, advanced AI-based threat detection, and facial recognition authentication.

REFERENCES

[1.] Singh R., Kumar A., "Secure Digital Evidence Management System," International Journal of Cybersecurity, 2019.
[2.] Patel S., Kumar P., "IoT Based Surveillance and Evidence Recording System," IEEE Conference on Smart Systems, 2020.
[3.] Zhang L., Wang Y., "Blockchain Based Digital Evidence Protection System," IEEE Access, 2021.
[4.] Stallings W., "Cryptography and Network Security," Pearson Education.
[5.] Forouzan B., "Data Communications and Networking," McGraw Hill.