Research Proposal:

Real-Time Detection and Mitigation of Frame Manipulation Attack Detection in Cyber security Systems

V. S. Suganya

Introduction

Surveillance cameras are critical components of modern security systems, providing real-time visual evidence for crime prevention, monitoring, and investigation. However, the integrity of video footage can be compromised through cyber attacks that manipulate or tamper with recordings. Such tampering includes frame injection, deletion, or replacement that can result in false evidence, loss of trust, and severe security consequences.

As surveillance systems increasingly rely on IP-based and cloud-connected technologies, they become vulnerable to cyber threats such as unauthorized access, malware infections, and video stream interception. Ensuring the authenticity and integrity of video footage is therefore an essential aspect of cyber security in surveillance environments.

This research aims to design a robust cyber security framework to detect, prevent, and respond to video footage tampering in surveillance systems using a combination of encryption, blockchain-based validation, and AI-driven tamper detection.

Problem Statement

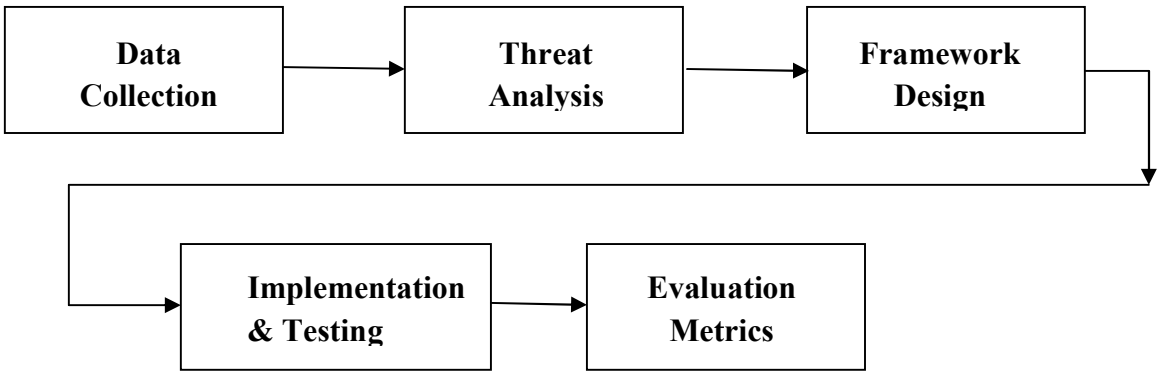
Traditional surveillance systems often prioritize storage and accessibility over data integrity. Attackers can exploit firmware vulnerabilities or insecure transmission protocols to alter or overwrite recorded footage without detection. Existing encryption or checksum methods are insufficient to guarantee real-time tamper detection in large-scale surveillance networks.

Therefore, there is a critical need for an intelligent and scalable cybersecurity mechanism capable of identifying tampered video data, verifying authenticity, and maintaining an immutable audit trail of surveillance footage.

Objectives

1. To identify the methods and types of video footage tampering in modern surveillance systems.
2. To analyze the vulnerabilities that enable unauthorized alteration or manipulation of video streams.
3. To develop algorithms capable of detecting tampering through visual inconsistencies and metadata anomalies.
4. To evaluate the effectiveness of the proposed framework through simulations or prototype implementation.

Methodology



Expected Outcomes

- A comprehensive taxonomy of tampering techniques and vulnerabilities in surveillance systems.
- A prototype demonstrating real-time tampering detection with high accuracy.
- Recommendations for secure deployment and maintenance of surveillance infrastructures.

Significance of the Study

The proposed research will strengthen the cyber security posture of surveillance systems by ensuring that captured footage remains tamper-proof and verifiable. This innovation can greatly enhance law enforcement reliability, judicial evidence credibility, and organizational data protection standards.

Additionally, the framework can be applied across smart city monitoring, banking security, transport surveillance, and critical infrastructure protection, ensuring trustworthy and resilient video security systems.