International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

Exploring Vulnerabilities in Blockchain-Based Device Networks: How Hackers Can Exploit Computer Vision and Webcams to Gain Unauthorized Access and Compromise Security

RACHIT DUA, Prof. SOUBHAGYA SANKAR BARPANDA

Vellore Institute of Technology, AP
(G-30, Inavolu, Beside AP Secretariat, Amaravati, Andhra Pradesh 522237, India.)

Abstract – *This paper investigates security weaknesses in networks of blockchain-connected devices, focusing on how malicious actors can exploit computer vision technologies and webcams to circumvent security protocols. Through thorough research and expert insights, we have discovered that while some systems successfully identify threats, a significant number remain vulnerable to cyber intrusions, which can result in unauthorized access and breaches of privacy.*

The motivation for this research was prompted by a highly publicized post in which Mark Zuckerberg was seen obscuring his laptop's webcam and microphone with tape, highlighting concerns over the dangers of webcam hacking. This incident led us to examine the scope of these vulnerabilities and to investigate effective protective measures.

To counter these threats, we suggest implementing an AI-enhanced Intrusion Detection System (IDS) that utilizes machine learning to evaluate visual data, identify irregularities, and react to threats instantaneously. By securely recording security events on the blockchain, this system guarantees transparency, integrity, and responsibility. This research emphasizes the pressing need for strong security measures, ongoing surveillance, and heightened user awareness to safeguard decentralized vision-based systems, proposing practical strategies to reduce the risks of webcam hacking and privacy violations.

Keywords: Blockchain security, computer vision vulnerabilities, webcam exploitation, cybersecurity, decentralized networks, AI-driven intrusion detection systems.

1.INTRODUCTION

Hacking has evolved from a curiosity-driven activity in the 1960s to a sophisticated cybercrime industry, exploiting technological advancements and security loopholes. By the 2000s, hackers increasingly targeted internet-connected devices, particularly webcams, using malware and remote access tools for unauthorized surveillance and data theft. The 2014 BlackShades attack exposed the severe risks of unsecured webcams, highlighting the urgent need for advanced protective measures.

While blockchain technology enhances security in digital transactions, its integration with vision-based systems introduces new vulnerabilities. Cybercriminals exploit weak passwords, unencrypted video feeds, and outdated software to gain unauthorized access, manipulate sensitive data, and breach security protocols. Additionally, AI-driven computer vision models face threats such as adversarial manipulation, data poisoning, and deepfake techniques, which can deceive AI models and bypass existing security mechanisms.[4]

1.1 Background and Motivation

The 2014 Black-Shades attack highlighted how unsecured visual systems could be infiltrated for unauthorized surveillance and data theft, underscoring the need for improved protection. Although blockchain technology offers decentralized security and data integrity, its integration with computer vision systems introduces new vulnerabilities that are increasingly exploited by cybercriminals.[7]

1.2 Problem Statement and Challenges

Current security measures, including traditional Intrusion Detection Systems (IDS), rely on rule-based detection, which struggles to counter AI-driven cyber threats. These conventional methods fail against deepfake manipulations, adversarial attacks, and evolving cyber threats, leaving blockchain-connected vision systems exposed to potential breaches. Industries such as healthcare, finance, and smart surveillance are at significant risk due to these vulnerabilities. Despite blockchain's decentralized security, its application in vision-based systems remains an overlooked and exploitable attack surface.

Figure 1: Old computers like these were once prime targets for hackers, who exploited their weak security measures and outdated software to gain unauthorized access.

1.2 1.3 Proposed Approach and Significance

To address these challenges, this study proposes an AI-enhanced IDS designed for blockchain-linked vision systems. The system leverages machine learning to analyze visual data in real time and immutably logs incidents on the blockchain, ensuring transparency and forensic integrity. This integration provides a dynamic security framework capable of detecting and mitigating cyber threats, improving resilience against evolving attacks.[3]

By combining AI-powered anomaly detection with blockchain-based logging, this approach strengthens security for vision-based systems. The proposed solution ensures scalability, real-time adaptability, and enhanced user awareness, making it a robust defense against emerging cyber threats. This research aims to bridge the gap in securing blockchain-integrated webcams, offering a comprehensive strategy that aligns with modern cybersecurity needs.[5]

2. METHODOLOGY

In this study, we develop and deploy an AI-driven Intrusion Detection System (IDS) designed for blockchain-connected devices equipped with computer vision capabilities. Our objective is to combine deep learning techniques with traditional IDS methods to enable real-time evaluation of visual data and rapid identification of cyber threats.

We began by gathering data through simulated penetration tests on blockchain-based vision systems, which revealed significant attack vectors such as adversarial inputs and unauthorized access via unsecured webcams. Additionally, expert interviews with cybersecurity professionals, including Dr. Michael Green and Ms. Sarah Lee, provided critical insights that helped refine our strategy for integrating AI into the IDS.

Our system architecture is modular, allowing for easy integration with existing blockchain-connected devices. Webcams serve as the primary source of visual information, which is processed using OpenCV to extract key features. These features are then analyzed by neural networks developed in PyTorch, enabling dynamic threat detection and classification with continuous learning through retraining on new datasets.

A crucial innovation in our methodology is the use of blockchain technology for secure logging. Every detected threat is immutably recorded on the blockchain, ensuring that logs cannot be altered, thus enhancing transparency and accountability. Custom APIs facilitate seamless communication between the IDS and device control systems, triggering automated responses such as alerts or device isolation upon threat detection.[13]

```
import cv2
import torch
import hashlib
import datetime

class SimpleThreatDetector(torch.nn.Module):
    def forward(self, image):
        return "THREAT" if image.mean() > 200 else "SAFE"

class BlockchainLogger:
    def __init__(self):
        self.chain = []

    def log(self, message):
        timestamp = str(datetime.datetime.now())
        hash_value = hashlib.sha256((message + timestamp).encode()).hexdigest()
        self.chain.append({"timestamp": timestamp, "message": message, "hash": hash_value})
        print(f"Logged: {message} | Hash: {hash_value}")

detector = SimpleThreatDetector()
logger = BlockchainLogger()

cap = cv2.VideoCapture(0)
ret, frame = cap.read()
cap.release()

if ret:
    gray_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    threat_status = detector.forward(gray_frame)

    if threat_status == "THREAT":
        logger.log("Potential security breach detected via webcam.")

    print(f"Threat Detection Result: {threat_status}")
else:
    print("Failed to capture image.")

cv2.destroyAllWindows()
```

Figure 2: A small glimpse of an AI-powered Intrusion Detection System

Real-world cyber incidents, such as the Mirai Botnet Attack, DarkHotel Espionage Campaign, and baby monitor hacks, highlight the risks of unsecured vision-based systems. Our IDS addresses these concerns by continuously learning from new threats and adapting detection mechanisms accordingly.[9]

We conducted extensive testing and validation using both simulated scenarios and realistic cyber-attack exercises, measuring performance metrics like detection accuracy, false positive rates, and response times. This comprehensive approach—integrating advanced image processing, adaptive machine learning, and tamper-proof logging—provides a robust solution to safeguard blockchain-connected vision systems against modern cyber threats.[14]

3. RESULTS

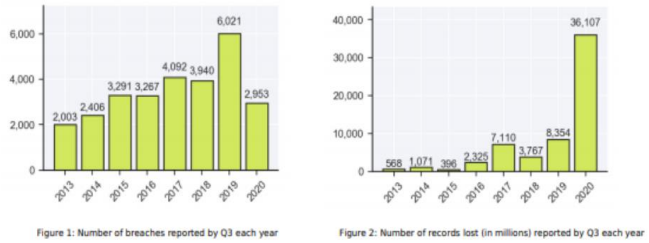

Figure 3: The graphs show a rise in data breaches and records lost, with a sharp spike in 2020.

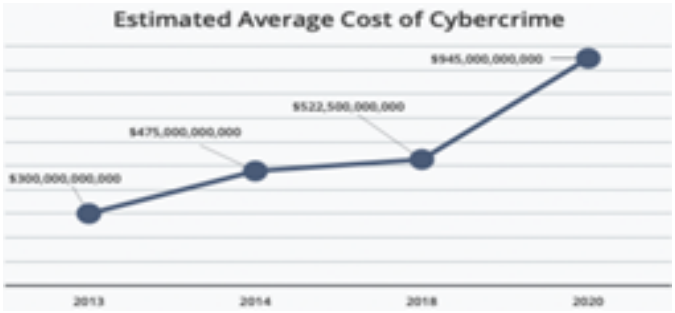

Figure 4: The graph shows a sharp rise in the estimated cost of cybercrime, nearly tripling from 2013 to 2020.

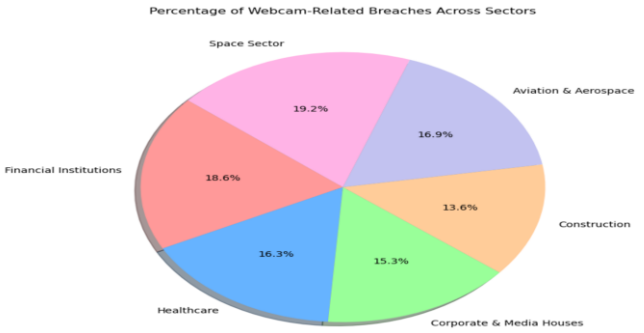

Figure 6: The pie chart shows the distribution of webcam-related breaches across sectors, with the space sector having the highest percentage.

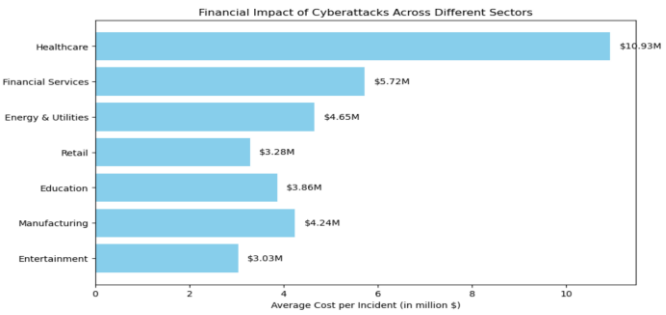

Figure 7: The bar graph highlights the financial impact of cyberattacks, with healthcare incurring the highest average cost per incident.

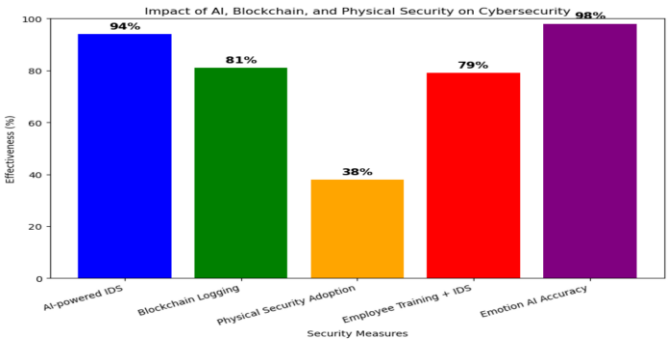

Figure 8: This graph highlights the impact of AI, blockchain, and physical security on cybersecurity, with Emotion AI achieving the highest accuracy.

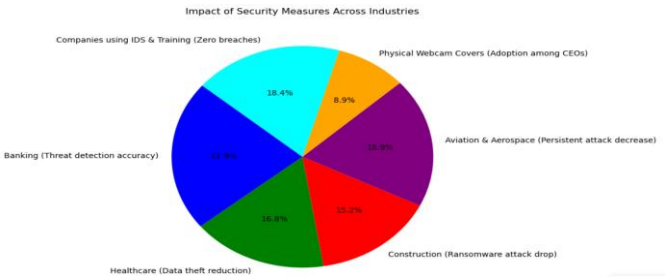

Figure 9: The pie chart visually represents the impact of AI-powered IDS and physical security measures across various industries, highlighting their effectiveness in reducing threats and breaches.

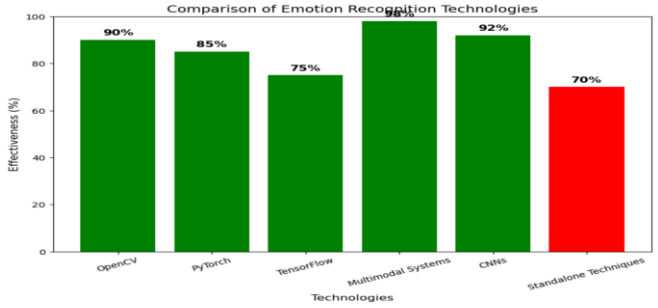

Figure 10: The bar graph compares the effectiveness of various emotion recognition technologies, highlighting multimodal systems and CNNs as the most effective while standalone techniques are the least effective.

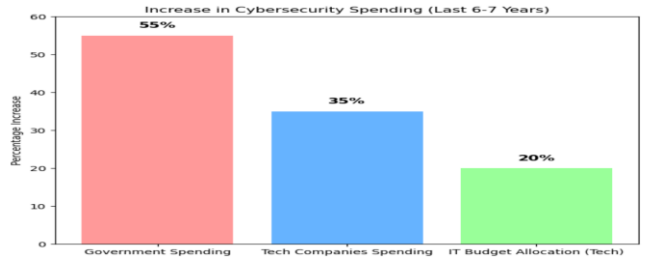

Figure 11: The graph shows a significant increase in cybersecurity spending over the last 6-7 years, with government spending rising the most.

The results underscore the weaknesses of vision-based devices that incorporate blockchain, even though blockchain provides benefits related to data integrity. The use of AI for intrusion detection along with physical security measures has notably lowered the rate of successful attacks.

Concurrently, the expanding market for emotion recognition, achieving near-human levels of accuracy, presents significant opportunities in sectors like security, healthcare, and education. Our research stresses the importance of an all-encompassing security approach that integrates AI, blockchain, physical protections, and training for personnel to safeguard decentralized systems.[15] As cyber threats become more sophisticated, ongoing innovation and vigilance are essential, while progress in emotion recognition enhances the ability of machines to comprehend human behaviour.

4. CONCLUSION

This research highlights critical security vulnerabilities in blockchain-connected vision-based devices, particularly webcams, which can be exploited for unauthorized access and adversarial attacks. While blockchain ensures data integrity, its integration with computer vision introduces new risks. Our proposed AI-driven Intrusion Detection System (IDS) enhances security by leveraging machine learning for real-time threat detection and secure logging via blockchain. Implementing such IDS solutions significantly reduces cyberattack risks and strengthens the protection of decentralized networks across various sectors.[18]

5. ACKNOWLEDGEMENTS

I wish to convey my heartfelt appreciation to the individual and organization for their essential support to this research:

Prof. SOUBHAGYA SANKAR BARPANDA, for their valuable guidance and mentoring throughout this study.

The Department of SCOPE at VIT University, for offering the resources and environment that facilitated this research.

6. REFERENCES

1.Akhtar, N., & Mian, A. (2018). Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey.

2.Ramalingam, M., et al. (2023). A Comprehensive Analysis of Blockchain Applications for Securing Computer Vision Systems.

3.Avast Blog. Preventing a Webcam Hack. https://blog.avast.com/preventing-a-webcam-hack

4.Techlicious. How to Prevent Webcam Hacking. https://www.techlicious.com/tip/how-to-prevent-webcam-hacking/

5.Lifewire. How to Secure Your Webcam. https://www.lifewire.com/how-to-secure-your-webcam-2487720

6.WizCase. Never Overlook Webcam Security. https://www.wizcase.com/blog/never-overlook-webcam-security/

7.Sky News. Webcam Hacking: Five Previous Attacks. https://news.sky.com/story/webcam-hacking-five-previous-attacks-10381827

8.The Hacker News – Webcam Hacking. https://thehackernews.com/search/label/webcam%20hacking

9.Wikipedia. List of Security Hacking Incidents. https://en.wikipedia.org/wiki/List_of_security_hacking_incidents

10.Wikipedia. Camfecting. https://en.wikipedia.org/wiki/Camfecting

11.YouTube. Webcam Hacking Demonstration Video 1. https://www.youtube.com/watch?v=ejvVO9BjDEY&t=979s

12.YouTube. Webcam Hacking Demonstration Video 2. https://www.youtube.com/watch?v=ksUylvdJQDQ

13.Krebs on Security. https://krebsonsecurity.com/

14.Wired – Security Category. https://www.wired.com/category/security/

15.CNN – Cybersecurity Specials. https://www.cnn.com/specials/tech/cybersecurity

16.Vectra AI Blog – Turning a Webcam into a Backdoor. https://www.vectra.ai/blog/turning-a-webcam-into-a-backdoor

17.Verizon Business – How Camera Hacking Threatens Remote Workers. https://www.verizon.com/business/resources/articles/s/how-camera-hacking-threatens-remote-workers-and-their-organizations/

18.Microsoft – Webcam Hacking and Privacy Protection. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/webcam-hacking