iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77032

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

Virtual Crime Scene Investigation and Emerging Future Crime Scene Paradigms: A Forensic and Criminological Perspective

Shashikiran V[1], Dr. Bharat JK[2]
[1]*Assistant Professor- Criminology & Forensic Science, Acharya Institutes, Bengaluru*
[2]*Teaching Assistant, Dept of Criminology and Forensic Science, Davangere University, Davangere Karnataka*

Abstract: ***The rapid digitization of society has fundamentally transformed the nature of crime and crime scene investigation. Traditional physical crime scenes are increasingly complemented or replaced by virtual and technology-driven environments, commonly referred to as Virtual Crime Scenes (VCS). Scholars have observed that digital environments now function as primary loci of criminal activity rather than merely auxiliary sources of evidence (Casey, 2011; Brenner, 2013). Alongside this shift, emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), blockchain, cloud computing, and metaverse platforms are shaping what can be described as future crime scenes. This paper critically examines the concept of virtual crime scenes, their investigative methodologies, evidentiary value, and legal admissibility, with a forward-looking analysis of upcoming and future crime scene paradigms. The study adopts a doctrinal and analytical approach, integrating forensic science, criminology, and legal frameworks, with specific reference to the Indian context under the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023. The paper further highlights technological, legal, and ethical challenges, and proposes strategic recommendations for law enforcement agencies and forensic institutions to effectively address crimes of the future.***

Keywords: Virtual Crime Scene, Digital Forensics, Cybercrime, Future Crime Scene, IoT Forensics, Artificial Intelligence, Metaverse Crime

I. INTRODUCTION

Crime scenes have traditionally been understood as physical locations where unlawful acts occur and where tangible evidence is collected. Classical forensic literature emphasizes spatial control, physical boundaries, and material traces as defining elements of crime scene investigation (Saferstein, 2018). However, the expansion of digital technologies, pervasive internet connectivity, and smart systems has significantly altered this classical understanding. Contemporary criminal investigations increasingly rely on data generated through computers, mobile devices, cloud infrastructures, and online platforms, where digital traces often provide the most probative evidence (Casey, 2011). The emergence of cybercrime, online financial frauds, digital sexual offenses, cyberstalking, and technology-assisted organized crime has necessitated the recognition of Virtual Crime Scenes (VCS) as independent investigative domains. According to Brenner (2013), cyberspace operates as a new social environment where traditional legal and criminological concepts of space and jurisdiction are continuously challenged. Furthermore, advancements in artificial intelligence, big data analytics, blockchain technologies, and immersive virtual environments indicate that future crimes will increasingly occur in complex hybrid ecosystems combining physical, digital, and virtual realities (Europol, 2023).

This paper aims to analyze the concept of virtual crime scenes and explore emerging future crime scene paradigms from a forensic and criminological standpoint, with particular emphasis on investigative challenges, evidentiary integrity, and legal admissibility.

II. CONCEPT AND NATURE OF VIRTUAL CRIME SCENE

A Virtual Crime Scene can be defined as a digitally created or digitally existing environment in which criminal activity occurs and where electronic evidence is generated, stored, transmitted, or manipulated. Unlike traditional crime scenes, virtual crime scenes lack fixed geographical boundaries and are often distributed across multiple servers, devices, and jurisdictions (Casey, 2011).

From a criminological perspective, virtual crime scenes represent socially constructed digital spaces where motivated offenders, suitable targets, and absence of capable guardians converge, aligning with routine activity theory in cyberspace (Yar, 2005). Technologically, VCS are characterized by their dependence on network infrastructures, software platforms, and data ecosystems.

A. Characteristics of Virtual Crime Scenes

1) Absence of fixed physical location
2) Dependence on electronic devices and network connectivity
3) Highly volatile and easily alterable evidence
4) Cross-border and multi-jurisdictional nature of offenses
5) Requirement of specialized technical and forensic expertise

B. Types of Virtual Crime Scenes

1) Pure Virtual Crime Scenes: Crimes occurring entirely in cyberspace such as hacking, phishing, ransomware attacks, online identity theft, and cryptocurrency scams (Wall, 2015).
2) Hybrid Crime Scenes: Crimes involving both physical and digital components, such as ATM skimming, cyber-enabled terrorism, GPS-assisted kidnappings, and online coordination of violent crimes (Europol, 2023).

III. DIGITAL EVIDENCE IN VIRTUAL CRIME SCENES

Digital evidence forms the backbone of virtual crime scene investigations. It includes any information of probative value stored or transmitted in digital form.

A. Sources of Digital Evidence

1) Computers and mobile devices
2) Cloud storage platforms
3) Social media and messaging applications
4) Network logs and IP records
5) IoT devices such as smart cameras and wearables

B. Nature of Digital Evidence

Digital evidence is fragile, easily duplicated, and susceptible to alteration. Therefore, maintaining integrity through hashing, write blockers, and proper chain of custody is essential for legal admissibility.

IV. INVESTIGATION OF VIRTUAL CRIME SCENES

Virtual crime scene investigation follows a structured forensic methodology adapted from traditional crime scene principles.

1) Identification and Preservation: Investigators must identify relevant digital assets and ensure preservation through isolation, imaging, and access control.
2) Collection and Examination: Forensic acquisition techniques such as disk imaging, logical extraction, and cloud data acquisition are employed. Examination includes timeline analysis, keyword searches, metadata examination, and malware analysis.
3) Analysis and Reconstruction: The final stage involves correlating digital events to reconstruct criminal behavior, intent, and sequence of actions.

V. EMERGING AND FUTURE CRIME SCENE PARADIGMS

The evolution of technology is expanding the concept of crime scenes beyond present virtual environments. Emerging technologies are expected to define future crime scenes that are increasingly autonomous, immersive, and data-intensive.

A. IoT-Based Crime Scenes

The proliferation of Internet of Things (IoT) devices has transformed homes, cities, and vehicles into continuous data-generating environments. Smart homes, wearable health devices, and intelligent transportation systems may serve as silent witnesses to criminal activity. IoT forensics involves the collection and analysis of sensor data, logs, and communication records, presenting challenges related to data heterogeneity and privacy (Zawoad & Hasan, 2015).

B. Artificial Intelligence and Algorithmic Crime Scenes

Artificial intelligence introduces crime scenes where algorithms themselves become instruments or targets of crime. Deepfake technologies, automated cyber-attacks, and AI-driven financial manipulation represent emerging threats. The forensic examination of training datasets, algorithmic decision trails, and model outputs will become critical in future investigations (Goodfellow et al., 2014; Europol, 2023).

C. Blockchain and Cryptocurrency Crime Scenes

Decentralized blockchain systems generate immutable transaction records, creating unique crime scenes embedded within distributed ledgers. Cryptocurrency-related crimes require forensic tracing of wallet addresses, transaction flows, and exchange logs, despite challenges posed by anonymity-enhancing technologies (Conti et al., 2018).

D. Metaverse and Virtual Reality Crime Scenes

Metaverse platforms introduce immersive virtual environments where crimes such as virtual sexual harassment, identity impersonation, financial fraud, and psychological harm may occur. These crime scenes raise complex questions regarding jurisdiction, victimization, and evidentiary representation of virtual conduct (Ball, 2022).

VI. LEGAL AND ETHICAL CHALLENGES

Virtual and future crime scenes present significant legal challenges related to jurisdiction, privacy, data protection, and admissibility of electronic evidence.

In India, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023, provide the legal foundation for electronic evidence, but continuous legal reform is necessary to keep pace with technological change.

Ethical concerns include mass surveillance, misuse of digital evidence, and violation of individual privacy rights.

VII. ROLE OF FORENSIC EXPERTS AND CAPACITY BUILDING

The investigation of virtual and future crime scenes requires highly trained forensic professionals with expertise in digital forensics, cyber law, data analytics, and emerging technologies. Continuous training, infrastructure development, and inter-agency cooperation are essential.

VIII. ADVANTAGES AND IMPORTANCE OF VIRTUAL AND FUTURE CRIME SCENES

The integration of virtual and future-oriented crime scene paradigms offers several significant advantages for modern criminal justice systems. These advantages enhance investigative efficiency, evidentiary accuracy, and preventive policing.

A. Advantages of Virtual Crime Scenes

1) Enhanced Evidence Availability: Virtual crime scenes generate large volumes of digital footprints such as logs, metadata, geolocation data, and transaction records, which can provide detailed reconstructions of criminal activities.
2) Non-Destructive Evidence Collection: Digital evidence can be duplicated without altering the original source, allowing repeated examination while preserving evidentiary integrity.
3) Time-Stamped and Automated Documentation: Most digital systems automatically record time, date, and user activity, reducing ambiguity and human error in crime scene documentation.
4) Remote Accessibility: Virtual crime scenes enable investigators to access and analyze evidence remotely, which is especially useful in cross-border and large-scale cybercrime cases.
5) Improved Crime Reconstruction: Digital timelines, communication logs, and behavioral analytics assist in precise reconstruction of criminal intent, planning, and execution.
6) Cost and Resource Efficiency: Compared to extensive physical crime scene operations, virtual investigations can reduce logistical costs and manpower requirements.

IX. IMPORTANT FEATURES OF EMERGING AND FUTURE CRIME SCENES

Future crime scenes are characterized by advanced technological integration, automation, and data-driven environments. These features will redefine investigative strategies.

1) Intelligent and Data-Rich Environments: Future crime scenes will be embedded with AI-driven systems capable of generating, storing, and analyzing vast datasets in real time, such as smart cities and intelligent transport systems.
2) Interconnected IoT Ecosystems: Crime scenes will involve multiple interconnected devices, including smart homes, vehicles, wearables, and surveillance systems, requiring multi-layered forensic correlation.
3) Predictive and Preventive Capabilities: Advanced analytics and machine learning models will assist law enforcement in predicting criminal behavior patterns and identifying high-risk activities before crimes occur.
4) Virtual and Immersive Spaces: Metaverse and extended reality platforms will create immersive environments where crimes can occur without physical contact, necessitating new evidentiary and jurisdictional frameworks.
5) Decentralized and Encrypted Structures: Blockchain-based systems and end-to-end encryption will make future crime scenes decentralized, anonymous, and resistant to traditional investigative methods.
6) Algorithm-Centric Evidence: Algorithms, source codes, AI decision logs, and training datasets will themselves become crucial forms of evidence in future investigations.
7) Cross-Jurisdictional Nature: Future crime scenes will routinely transcend national boundaries, increasing the importance of international legal cooperation and harmonized cyber laws.

X. EXPANDED ADVANTAGES OF VIRTUAL AND FUTURE CRIME SCENES

A. *Strategic and Operational Advantages*

1) Real-Time Monitoring and Response: Integration of live network monitoring, AI surveillance, and sensor-based alerts enables faster detection and response to criminal activities.
2) Evidence Permanence: Cloud backups, blockchain timestamping, and distributed storage increase the longevity and traceability of evidence.
3) Behavioral and Psychological Profiling: Digital footprints allow advanced offender profiling using criminological and behavioral analytics.
4) Cold Case Reinvestigation: Archived digital data can be reanalyzed using improved forensic tools, aiding reopening of unsolved cases.

B. *Advantages for Criminal Justice Administration*

1) Higher Conviction Support: Corroborated digital evidence strengthens prosecution cases.
2) Judicial Transparency: Electronic records, logs, and audit trails assist courts in objective decision-making.
3) Victim Protection: Cyber documentation supports victims of online harassment, stalking, and financial frauds.

C. *National Security Advantages*

1) Counter-Terrorism Support: Monitoring of encrypted communications, online radicalization, and digital financing networks.
2) Border and Defense Security: Satellite data, drone surveillance, and cyber intelligence contribute to proactive defense strategies.

XI. LEGAL FRAMEWORK, COURTS, AND APPLICABILITY WITH CASE LAWS

A. *Indian Legal Framework*

1) Information Technology Act, 2000 – Sections 43, 65, 66, 66C, 66D, 67 dealing with unauthorized access, data tampering, identity theft, cheating by personation, and publication of obscene digital content.
2) Bharatiya Nyaya Sanhita (BNS), 2023 – Recognition of cyber-enabled and technology-facilitated offenses.
3) Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 – Procedures for search, seizure, investigation, and preservation of electronic evidence.
4) Bharatiya Sakshya Adhiniyam, 2023 – Legal recognition, admissibility, integrity, and authentication of electronic evidence including hash values and digital records.

B. *Landmark Indian Judicial Decisions on Virtual Crime Scenes*

1) State (NCT of Delhi) v. Navjot Sandhu (Parliament Attack Case), (2005): The Supreme Court recognized the evidentiary value of electronic records such as call detail records (CDRs) and digital communication, highlighting the importance of proper collection and authentication of electronic evidence.

2) Anvar P.V. v. P.K. Basheer, (2014): The Supreme Court held that electronic evidence is admissible only when accompanied by the mandatory certification, reinforcing procedural safeguards in virtual crime scene investigations.
3) Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020): The Court clarified the mandatory nature of certification for electronic evidence while also recognizing practical exceptions, strengthening the framework for admissibility of digital forensic evidence.
4) Shreya Singhal v. Union of India, (2015): This landmark judgment balanced cyber regulation with fundamental rights, emphasizing the need for lawful and proportionate investigation of online content.
5) P. Gopalkrishnan v. State of Kerala, (2020): The Supreme Court emphasized the accused's right to access electronic evidence, underscoring transparency and fair trial principles in digital investigations.

C. International Judicial Perspectives

1) R v. Sheppard (UK): The court accepted computer-generated evidence, emphasizing reliability and system integrity, influencing global standards in virtual crime scene analysis.
2) United States v. Comprehensive Drug Testing, Inc. (USA): The case highlighted judicial oversight in digital searches and seizure of electronic data, stressing proportionality in virtual crime scene investigations.

D. Applicability in Courts

These judicial pronouncements demonstrate that virtual crime scene evidence is now routinely relied upon by trial courts, High Courts, and the Supreme Court of India, provided procedural safeguards, forensic integrity, and expert testimony requirements are fulfilled.

XII. ROLE OF POLICE, MILITARY, AND SPECIALIZED FORCES

A. Indian Police and Security Agencies

1) Cyber Crime Police Stations under State Police
2) Indian Cyber Crime Coordination Centre (I4C)
3) Central Bureau of Investigation (CBI) – Cyber and economic offenses
4) National Investigation Agency (NIA) – Cyber-terrorism and digital radicalization
5) State and Central Forensic Science Laboratories (SFSL & CFSL)

B. Military and Paramilitary Role (India)

1) Indian Army Cyber Operations Units
2) Defence Cyber Agency (DCA)
3) Central Armed Police Forces (CAPFs) for cyber-assisted internal security
4) Military Intelligence & Signals Units for cyber warfare and intelligence

C. International Police and Military Agencies

1) INTERPOL Cybercrime Directorate
2) EUROPOL – European Cybercrime Centre (EC3)
3) FBI Cyber Division (USA)
4) NSA and US Cyber Command
5) UK National Crime Agency (NCA)

These agencies collaborate on intelligence sharing, cyber defense, and transnational investigations.

XIII. TECHNOLOGICAL TOOLS, DEVICES, AND SAFETY INFRASTRUCTURE FOR VIRTUAL AND FUTURE CRIME SCENES

A. Digital Forensic Tools (Software)

1) Disk and Memory Forensics: EnCase, FTK, Autopsy, X-Ways Forensics
2) Mobile Forensics: Cellebrite UFED, Oxygen Forensic Detective, MSAB XRY
3) Network and Cloud Forensics: Wireshark, NetworkMiner, AWS Forensics Toolkit, Azure Security Center
4) Malware and Cyber Analysis: IDA Pro, Ghidra, Volatility Framework, Cuckoo Sandbox

5) Blockchain and Cryptocurrency Forensics: Chainalysis, CipherTrace, Elliptic
6) OSINT and Social Media Analysis: Maltego, Social Links, SpiderFoot

B. Hardware Devices and Equipment
1) Forensic workstations (high-RAM, multi-core processors)
2) Write blockers (hardware and software-based)
3) Faraday bags and Faraday boxes
4) Forensic duplicators and disk imagers
5) Network taps and packet capture devices
6) Secure evidence storage servers

C. Computers and Specialized Systems
1) Air-gapped forensic computers
2) High-performance servers for big data analysis
3) GPU-based systems for AI and deepfake analysis
4) Virtual machines and sandbox environments

D. Mobile, IoT, and Emerging Devices
1) Smartphones (Android, iOS) for test and validation
2) IoT devices (smart cameras, smart speakers, wearables)
3) Vehicle infotainment systems and GPS units
4) Drones and UAV data extraction tools

E. Safety, Security, and Integrity Measures
1) Hashing tools (MD5, SHA-1, SHA-256)
2) Access control and role-based authentication
3) Chain of custody documentation systems
4) Digital evidence management systems (DEMS)
5) Encrypted storage and secure backups

F. Police, Military, and Institutional Infrastructure
1) Cyber Crime Police Stations and Cyber Labs
2) Central and State Forensic Science Laboratories (CFSL/SFSL)
3) Defence Cyber Agency forensic infrastructure
4) Intelligence fusion centers and SOCs
5) International collaboration platforms (INTERPOL I-24/7)

G. Training and Human Resource Requirements
1) Certified Digital Forensic Examiners (CDFE)
2) Cyber forensic analysts and SOC operators
3) Continuous skill upgradation in AI, IoT, and cloud forensics

XIV. RECOMMENDATIONS

1) Strengthening digital forensic laboratories and cybercrime units
2) Updating legal frameworks to address emerging technologies
3) Specialized training in AI, IoT, and blockchain for investigators
4) International cooperation for cross-border cybercrime investigation
5) Development of standard operating procedures for future crime scenes

XV. CONCLUSION

"In essence, virtual crime is old wine served in a technologically new bottle."

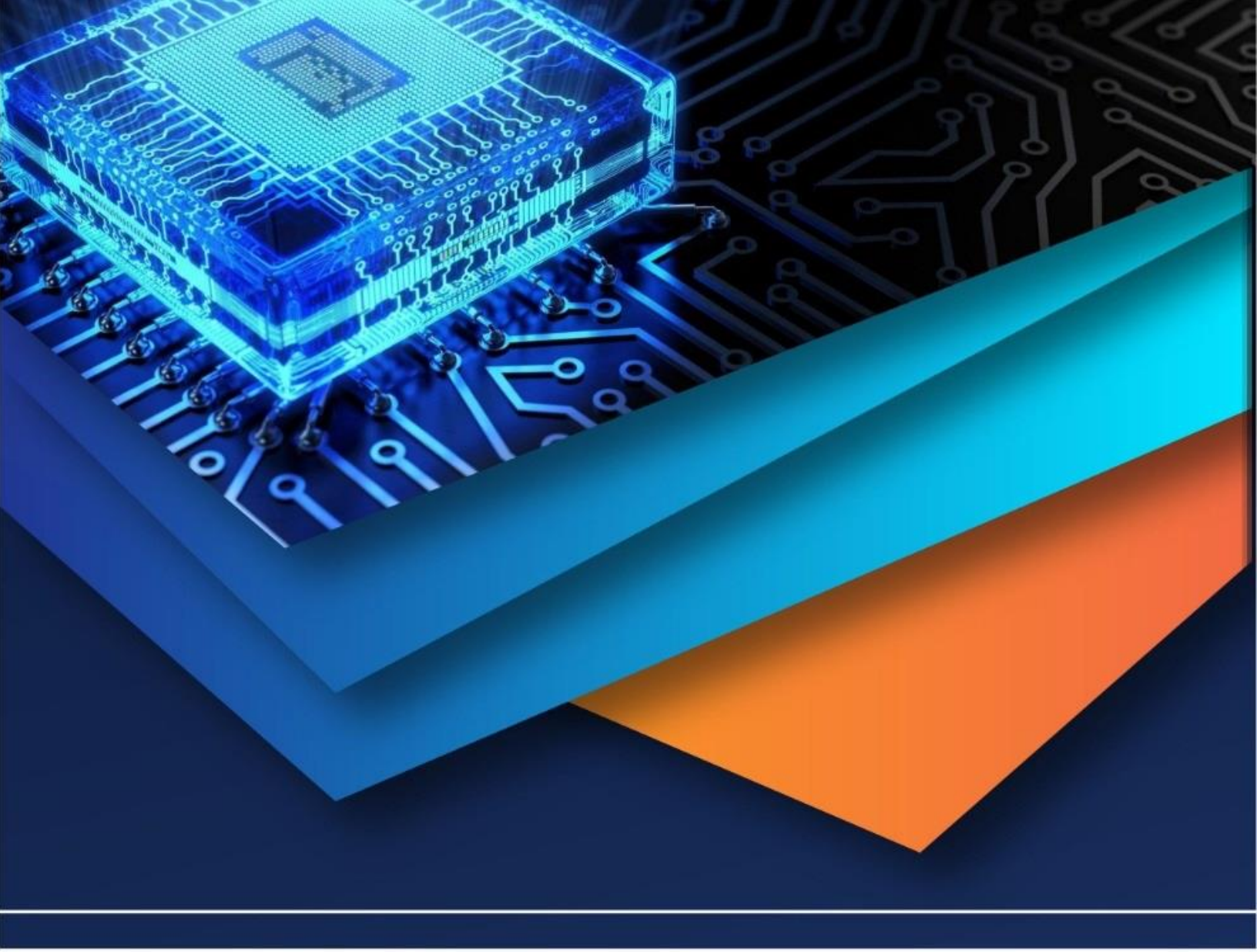
This study demonstrates that while criminal intent, motive, and behavioral patterns remain largely unchanged, the environments in which crimes are committed have undergone a profound transformation. Virtual and future crime scenes—ranging from cyberspace and cloud ecosystems to IoT networks and metaverse platforms—represent an evolutionary shift in the locus of crime rather than a fundamental change in its nature. The transition from physical to digital and hybrid crime scenes necessitates corresponding advancements in forensic methodologies, legal interpretation, and institutional preparedness.

The effectiveness of criminal justice responses in the digital age will depend on the ability of law enforcement agencies, forensic experts, policymakers, and courts to adapt traditional investigative principles to technologically mediated environments. Strengthening digital forensic capacity, updating legal frameworks, fostering inter-agency and international cooperation, and investing in continuous training are essential to ensure accountability and justice. As crime continues to adapt to new technological vessels, proactive policy implementation and scientific preparedness will remain central to addressing the challenges posed by virtual and future crime scenes.

REFERENCES

[1] Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.
[2] Carrier, B. (2005). File system forensic analysis. Addison-Wesley.
[3] Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to computer forensics and investigations (6th ed.). Cengage Learning.
[4] Rogers, M. K. (Ed.). (2016). Digital forensic investigation: A guide to evidence collection, analysis, and presentation. CRC Press.
[5] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
[6] Behl, A., & Behl, K. (2017). Cyberwar: The next threat to national security. Oxford University Press.
[7] Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Praeger.
[8] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038.
[9] Europol. (2022). Internet organised crime threat assessment (IOCTA). Europol Publications.
[10] Interpol. (2021). Global cybercrime strategy. Interpol.
[11] Chawla, M., & Sharma, S. (2020). Cybercrime investigation in India: Challenges and opportunities. Indian Journal of Criminology, 48(2), 55–68.
[12] Mittal, S. (2019). Digital evidence and Indian criminal justice system. Journal of Indian Law Institute, 61(3), 389–410.
[13] Singh, V. (2021). Admissibility of electronic evidence under Indian law. SCC Journal, 4, 112–128.
[14] Supreme Court of India. (2014). Anvar P.V. v. P.K. Basheer, AIR 2015 SC 180.
[15] Supreme Court of India. (2020). Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[16] Supreme Court of India. (2015). Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[17] Supreme Court of India. (2005). State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[18] Supreme Court of India. (2020). P. Gopalkrishnan v. State of Kerala, (2020) 9 SCC 161.
[19] Clough, J. (2015). Principles of cybercrime. Cambridge University Press.
[20] Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.
[21] Maras, M.-H. (2015). Computer forensics: Cybercriminals, laws, and evidence. Jones & Bartlett.
[22] Goodman, M. (2015). Future crimes. Doubleday.
[23] United Nations Office on Drugs and Crime. (2021). Handbook on cybercrime investigation. UNODC.
[24] National Institute of Justice. (2018). Digital evidence forensic standards. U.S. Department of Justice.
[25] R v. Sheppard [1993] AC 380 (UK).
[26] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).
[27] Sood, A. K., & Enbody, R. J. (2014). Targeted cyber attacks. Syngress.
[28] National Cyber Security Centre (UK). (2020). Cyber forensics and incident response. NCSC Publications.
[29] Jain, R., & Gupta, M. (2022). IoT forensics: Emerging challenges. International Journal of Digital Crime and Forensics, 14(1), 1–18.
[30] Kaur, H., & Kaur, P. (2021). Deepfake technology and criminal misuse. Journal of Cyber Law, 9(2), 77–95.
[31] Defence Cyber Agency. (2023). Cyber security doctrine of India. Ministry of Defence, Government of India.
[32] Indian Cyber Crime Coordination Centre (I4C). (2022). Cybercrime trends and responses in India. Ministry of Home Affairs.
[33] Bharatiya Sakshya Adhiniyam, 2023. Government of India.
[34] Bharatiya Nagarik Suraksha Sanhita, 2023. Government of India.
[35] Information Technology Act, 2000. Government of India.

***



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY