NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

# DIGITAL FORENSICS AND CCTNS: UNLOCKING THE FUTURE OF CRIME DETECTION

**Vanshika Shukla**

***Abstract:*** *Although the integration of digital forensics technologies with the criminal and criminal tracing network and systems (CCTNS) is a revolutionary change in the functioning of the Indian criminal justice system. The paper addresses the digital forensics transformation in terms of investigative practices and discusses how its association with the CCTNS improves the availability of real-time data, and the creation of inter-service cooperation and evidence-based policing. Digital forensics may be essential in combating cybercrime and financial fraud, because of its ability to collect, process and protect electronic evidence. The CCTNS operates under the national e-Government plan as a comprehensive online resource, operating with almost 15,000 police stations across the country, improving efficient communication networks. By combining their capabilities, digital forensics and CCTNS allow for faster detection of crimes, faster investigation and a higher resolution rate.*

*The study examines effective case studies, discusses the tools used and raises issues such as data privacy, legal recognition and the weaknesses of the IT and CCTNS infrastructure. In addition, it analyses the ethical aspects and defines the policy requirements for successfully implementing the digital transformation in the area of crime prevention. In sum, the study shows that India's future in crime detection rests on a robust technological structure, with digital forensics and CCTNS, for faster, cleaner and accountable justice outcomes.*

***Keywords:*** *Digital Forensics, Crime and Criminal Tracking Network and Systems (CCTNS), Cybercrime Investigation, Digital Evidence, Law Enforcement Technology.*

## I. INTRODUCTION

The development of digital technologies has transformed the reality of illegal activities and law enforcement challenges. The rapidly evolving nature of today's crimes, and in particular cybercrime, requires that investigative techniques are supplemented by more sophisticated investigative techniques. In these cases, forensic technology in digital form has become essential for the detection, capture, preservation and analysis of data related to online crimes. Perhaps, during these events, the Indian government launched the Criminal and Criminal Tracking Network and Systems (CCTNS), which aims to establish a basic, nationwide system for tracking and tracing criminals and criminals in a centralised format. The merging of the digital forensics and CCTNS is an important step towards creating a more efficient, open and technologically driven criminal justice system.

However, this study aims to critically examine the role of digital forensics in modern criminal investigations and to examine how it improves law enforcement effectiveness. The purpose of this study is to examine the CCTNS technology format and working methods; to determine the efficiency of digital forensics tools when integrated with centralised databases and to identify institutional, legal and technical challenges encountered during their deployment. One of the main points of this study is to determine the transformational impact of the practice of integrating digital forensics with CCTNS on the detection of crime, collection of evidence and prosecution.

Furthermore, the study, which focuses on rigorous analysis, is illustrated through real-life examples and policy assessments to explain the evolving relationship between digital forensics and CCTNS. The aim of this study is to identify key strengths and weaknesses in order to provide practical advice to decision-makers in order to improve the infrastructure and to support the coordination of the Agency's functions. In keeping with this it organised by theme, research starts with key concepts, continues to discuss technological applications and challenges, and finally discusses the trends and possible solutions.

## II. DIGITAL FORENSICS

Digital forensics involves a well organised approach to the search, extraction, storage and analysis of stored electronic information that can withstand the test of presentation to a court. Because digital companies now enable communication, financial transactions,

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

organizational processes and governmental functions, studying the patterns of electronic devices is crucial to the detection of criminal activities. Through digital forensics, investigators can obtain key data from computers, mobile devices, servers and storage systems, cloud platforms and embedded systems, revealing the motives and methods of the perpetrators of these crimes.

Several distinct areas of digital forensics have emerged, depending on the type of source material. In computer forensics, investigators examine computers and portable devices to retrieve data that has been erased or encrypted. Mobile forensics is the study of mobile phones and tablets, which provide information such as call history, texts and location, and updates from social networking sites. Network forensics is the capture and analysis of data flows on networks to detect signs of cyber-attacks and security incidents. Cloud forensics is responsible for identifying and examining evidence stored in a cloud environment, which requires specific tools and ideas of applicable law. Specific areas such as database forensics, e-mail forensics and malware forensics are necessary, specifically targeting unique digital artefacts relevant to specific types of crime.

Although, the importance of the digital forensics discipline is underlined by the evidence it provides, which is carefully verified and accompanied by precise time stamps; it is also tamper-proof, thus supporting claims in court proceedings. In keeping with this its value is crucial in many investigative fields, including cybercrime, financial fraud, data leakage, intellectual property theft, terrorism, and even traditional crimes with digital evidence. Through digital forensics, law enforcement can precisely identify the chronological order of events, the source of digital communications and the links between suspects and their criminal activities.

The chain of custody is part of digital forensics and ensures that evidence is stored and properly documented throughout the investigative process. evidence that all information is still intact and reliable; and the ability of the evidence to comply with legal requirements for use in court. Moreover, the digital forensics discipline stresses the use of specific tools, data extraction and interpretation programmes, while respecting international guidelines and promoting legal requirements. Digital forensics in the modern digital environment plays an important role in both criminal investigations and the accountability of public authorities, while maintaining public trust.

## III. CCTNS OVERVIEW

The Crime and Criminal Tracking Network and Systems (CCTNS) is a prominent e-Governance initiative of the Government of India which created by Ministry of Home Affairs under National e-Governance Program in 2009. The main objective of CCTNS, is to create an integrated information system for policing by digitization and linking of police stations and offices at higher-levels in the country. However, the goal of CCTNS, is to enhance the efficiency and the effectiveness of policing to enhance accessible real-time crime and criminal departments to authorities to support the immediate tracking, investigation, and crime control. Under the leadership of the National Crime Records Bureau (NCRB), the effort targets comprehensive national database of crime and criminals which will be accessible to the police departments across the country.

Though, CCTNS major role entails the integration of not less than 15,000 police stations and more than 6000 administrative organs such as district/state heads, forensic labs, jails, trials etc. The main objective of the platform is to automate the functions of FIR registration, investigation, charge sheet filing, and management of criminal records. The online conversion of these procedures in CCTNS is aimed at limiting manual bureaucracy, enhance levels of transparency, and assist streamline the flow of delivering criminal justice services. CCTNS has one of its best features in the citizen portal that provides citizens with the option to file complaints, request verification certificates, monitor progress on their FIRs, and receive more online police services, all arriving at the final goal of increasing transparency and citizen participation.

In addition, it enforces role-based access controls and a data privacy protection regime which restricts access to sensitive data to authorised persons only. The CCTNS also facilitates cross-border information sharing, which is essential to monitor transnational and organised crime activities. The CCTNS supports the strengthening of the national security and intelligence apparatus through enhanced cooperation with the national police and the national intelligence services. The integration of CCTNS with the National Intelligence and Digital Forensics databases greatly improves its practical application in proactive policing and profiling.

The CCTNS goes beyond a technological change; it means a change in the way the

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

criminal justice system in India is administered. CCTNS offers elements of speculative tools that rely on data mining and crime trends for police forces; thus, it supports informed decision-making and the pursuit of proactive policing approaches. The CCTNS fundamentally operates on the principles of preventive policing in contrast to the previous reactive model and plays an important role in the establishment of a digitally inclusive policing system with a public service focus. As the system develops further, the integration of technologies such as artificial intelligence and digital forensics will transform the practice of crime detection and law enforcement in India.

## IV. FORENSICS + CCTNS

Digital forensics and CCTNS play an important role in the modern delivery of criminal justice, system independently but in complementarity to help identify and investigate criminal offences. Digital forensics is concerned with the examination and preservation of digital artefacts, whereas CCTNS is the single platform for the organisation, management and use of crime and criminal data by law enforcement. Forced by the combination of these solutions, it represents a shift from isolated manual operations to a combined digital approach to the conduct of criminal investigations. Both systems have common goals to improve accuracy, use data to guide selection, and speed up the process of discovery. While digital forensics focuses on investigation and discovery of evidence, CCTNS is an administrative system, all about centralised storage and instant sharing of data relevant to crime and criminal activity within law enforcement organisations.

The effectiveness of these systems is achieved through a partnership model, where collected forensic evidence from digital sources such as IP addresses, encrypted materials or recovered deleted files are entered in the CCTNS database for further analysis. The result is better pattern identification, more creative characterisation of criminals and better tracking of multiple-agency cases. For example, developments in mobile forensics allow for the extraction of contact lists and movement patterns, which can then be synchronised with CCTNS data to reveal the links between people and crimes. However, there is integration, but each system still has its own specific responsibilities. Digital forensics requires a high level of technical skills and detail - individual evidence at this level, whereas the CCTNS controls general data systems and law enforcement at a systems level.

The core of the integration is real-time data integration, controlled by roles, the interoperability of digital evidence, and the interconnection of departments and states for operational purposes. The main function of digital forensics is to obtain digital evidence that is fit for trial, and the CCTNS will be a useful tool for the storage and dissemination of such evidence. This cooperation helps to carry out more effective predictive policing, improves case closure and improves accountability. However, integration raises important issues of data privacy, ethical aspects of surveillance and the admissibility of digital evidence in court. However, the introduction of digital forensics and CCTNS, empowering law enforcement and judicial authorities to build a more empowered system, speeding up the resolution of cases and a citizen-centric criminal justice system are important factors for India's emergence.

## V. TOOLS & TECHNIQUES

The platform that underpins effective cooperation between digital forensics and CCTNS is a good combination of tools and processes to support the acquisition, preservation, interpretation and dissemination of digital evidence. Key tools are needed to extract critical information from electronic devices and integrate it into centralised databases for meaningful analysis. The classification of digital forensics tools depends largely on the information that they generate for the purpose of their analysis. Software solutions such as EnCase and Forensic Toolkit are common in this practice and provide advanced forensic imaging and analysis capabilities for digital storage devices. Autopsy is an open source platform with a graphical user interface that allows users to explore hard drives, restore files, and investigate timelines. Perhaps, Cellebrite UFED, XRY and Oxygen Forensic Suite are mobile devices forensic tools used to extract SMS messages, call records, application information and GPS traces from smart phones, which are essential for digital footprints.

Software like Wireshark provides real-time monitoring of network packets in network forensics, while NetworkMiner is good for passive logging and session reconstruction. These tools help uncover illegal access, software viruses that are infiltrating networks, or unusual exchanges that may be evidence of cyber or conventional crime. Forensic analysis of databases and e-mails can be performed with applications such as SQLSuspect and MailXaminer, which are designed to detect

illegal changes, detect deleted e-mails and investigate the flow of communication. These tools are integrated into the CCTNS database, providing a structured repository of offences, FIRs, arrests, CHF and police records.

The tools and techniques in CCTNS are based on data standardisation, integration and real-time synchronization. The system has inherent capabilities such as: national search to enable cross-border access to crime data and create criminal profiles by comparing forensic reports with data on the perpetrators. It also includes role-based dashboards, crime mapping through GIS and automated reporting functions, which will increase efficiency and create greater transparency. The CTNS is also seeing a greater uptake of artificial intelligence, facial recognition and biometric matching technologies, which support predictive policing and enhanced surveillance.

Though, combined, these methods not only develop the investigative process itself, but also provide an effective, secure and scalable system for the treatment of digital evidence. When digital forensics and CCTNS are combined, law enforcement can monitor live communication of ongoing investigations, drive fast convictions and increase inter-agency cooperation in complex crimes.

## VI. CASE STUDIES

The Crime and Criminal Tracking Network and Systems (CCTNS), launched in 2009 with a budget of 2,000 crores, is a transformative e-government initiative linking more than 14,000 police stations across the country. In keeping with this as per record in 2022, it has reached a 100 percent coverage of 17,130 stations, digitizing first information reports (FIRs), investigative records and charging lists. The NCRB uses the CCTNS to produce an annual report on crime in India, which provides a comprehensive picture of crime trends. The 2022 report details registered and unsolved cases, reflecting the interaction of digital forensics and CCTNS in the modernisation of the Indian criminal justice system.

According to 2022, the number of cognizable crimes in India summed up to 5,824,946, divided into 3,561,379 cases under Indian Penal Code (IPC) and 2,263,567 cases under the This was a decline of 4.5%, from the previous year's total, meaning a drop-in crime by 5.3% per 100000 people (from 445.9 to 422.2), which meant that more correct population numbers were used. Moreover, Uttar Pradesh had the highest number of IPC crimes in the country with 753,675 followed by Maharashtra and Madhya Pradesh while Tamil Nadu topped in SLL reports, with Gujarat and Karnataka coming second. Specific crime categories included:

- Crimes Against Women: There were 445,256 reported cases during 2022, which was a 4% increase from the 428,278 cases reported in 2021 with cruelty by family members or husbands, kidnapping and abduction, assault to outrage modesty, and rape.
- Crimes Against Children: There were 162,449 incidents reported, the high numbers of which involved kidnapping, abduction.
- Other Key IPC Crimes: Murder (49.220), Rape (44.785), Kidnapping and Abduction (181.240), and Hurt (858.8).

These numbers, collected through CCTNS, reflect the effectiveness of the system in obtaining all-encompassing information about crime facilitate targeted approaches to law enforcement. Police statistics define closure of a case as the end of the investigation, where it can be closed by submission of a charge sheet or where it is formally closed. Unemployment for 2022 The police have officially closed the 3rd discontinued dormant theorem Remarkably, 71.3 of all IPC cases opened for investigation resulted in indictments, which indicates that this percentage led to indictments. The information provided on settled SLL cases was insufficient, although the high level of the charge sheets for specific legislation, such as the Excise Code, 99.2 percent, suggests a more rapid resolution of the infringements. Detailed resolution data for key crimes includes:

| Crime Head | Registered Cases | Charge-Sheeted | Charge-Sheeting Rate (%) |
|---|---|---|---|
| Murder (IPC) | 49,220 | 25,658 | 81.5 |
| Rape (IPC) | 44,785 | 26,508 | 77.9 |
| Kidnapping & Abduction (IPC) | 181,240 | 41,656 | 36.4 |
| Hurt (including acid attack, IPC) | 858,817 | 570,027 | 89.9 |
| Rioting (IPC) | 67,739 | 34,963 | 86.6 |
| The Excise Act (SLL) | 404,555 | 365,264 | 99.2 |
| Narcotics Drugs Act, 1985 (SLL) | 158,267 | 105,547 | 98.3 |
| The Arms Act (SLL) | 96,432 | 79,743 | 98.5 |

State-wise, Kerala (96.0%), Puducherry (91.3) and West Bengal (90.6) had the highest rates of IPC offences, reflecting effective investigative practices.

CCTNS helps to expedite case resolution as it allows real-time access to data, which could help

NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

the police to monitor investigations, share inter-state information leveraging systems such as Cri-MAC and produce analytical reports. Digital forensics supplements this by examining the electronic evidence which is important in cases such as cyber-crimes or high- level cases. For example, in the case of Himachal Pradesh, CCTNS has reduced the time for verification of passport from 70 days to 24 hours and enhanced the recovery rate of missing persons (85 % among women and 95 % among children), to demonstrate its effects.

Although details of exact pendency rates for 2022 are not completely laid bare, lower charge-sheeting rates for such crimes as kidnapping (36.4%) hint at increased pendency caused by complications of investigation. The rate of pendency of the economic crimes was 77.3% in Chandigarh 2021 and it shows continuous problems. Partial data from states such as Nagaland make it more complicated to analyse pendency. Inter-Operable Criminal Justice System (ICJS) that will combine CCTNS with e-Courts and e-Prisons will help in minimizing pendency through process management.

The 4.5 percent drop in registered crime between 2011 and 2022 is in line with the historical accumulation of cognisable offences (from 0.6 million in 1953 to 5.8 million in 2022), which continues to be driven by the tendency to increase the number of people who are involved in crime more than the number who are involved in crime (ORF crime). Crimes against women increased by 4 percent, indicating a serious problem of gender profiling. The high level of charging (SLL crimes) shows the efficient treatment of regulatory cases, but higher levels of charging (IPC crimes) require more investigation.

Based on CCTNS and NCRB data for 2022 show a registered crime rate of 5,824,946 and the number of indictments issued by the police is 3,660,786, representing a 71.3 percent indictment rate. Differentiation rates for different types of crime exist, and countries require targeted deterrence. CITES and digital forensics are the main pillars for improving case management, but delays and gaps are also essential for a strong justice system.

| Category | Registered Cases | Cases Disposed (IPC) | Charge-Sheeted (Selected) | Charge-Sheeting Rate (%) |
|---|---|---|---|---|
| Total Cognizable Crimes | 5,824,946 | 3,660,786 (IPC) | - | 71.3 (IPC) |
| Murder | 49,220 | Not Specified | 25,658 | 81.5 |
| Rape | 44,785 | Not Specified | 26,508 | 77.9 |
| Crimes Against Women | 445,256 | Not Specified | Not Specified | Not Specified |
| Crimes Against Children | 162,449 | Not Specified | Not Specified | Not Specified |

## VII. IMPLEMENTATION CHALLENGES

The integration of digital forensics with the CCTN has significantly improved the capabilities of law enforcement in India, although it has not been without its challenges. One of the main obstacles is the lack of sufficient infrastructure and resources in most police stations, particularly in cases involving rural and underdeveloped areas. Although CCTNS has been deployed in over 15 000 police stations, many of these police stations lack the technological equipment such as fast internet connection, modern computer systems and storage systems that are necessary for the smooth functioning and interoperability of digital forensics tools. The lack of a strong infrastructure limits the effectiveness of both digital forensics and CCTNS, resulting in delays in the processing of cases and obtaining data.

Another major problem is the lack of skilled staff. Digital forensics is a process requiring expertise in areas such as data mining and analysis, and cyber-security. However, law enforcement agencies are having difficulty recruiting and retaining trained digital forensics professionals. In addition, the training of existing officers in new forensic tools, technologies and investigative methods should be continued. The disparity in computer skills is exacerbated by the ever-changing nature of technology, with cyber criminals constantly evolving to new ways of doing things that are hard to maintain.

Interoperability problems between CCTNS and other national or regional databases are also a problem. Although the CCTNS should be interoperable, most police stations at national level are operating on legacy systems or incompatible software, which makes data synchronization between different jurisdictions impossible. These integration gaps hinder the efficiency of sharing, reducing the logical response capacity of law enforcement organisations to work effectively in cross-border cases.

However, legal and ethical issues in the work with digital evidence are another issue. The combination of digital forensics and CCTNS also raises important questions about data privacy, chain of custody and the admissibility

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

of digital evidence in court. There is no uniform national system for the handling and documentation of digital evidence, which may compromise the integrity of investigations and make the presentation of digital evidence in court difficult.

The issue of confidentiality is also important. The more data collected, the more sensitive the information becomes to be classified. Both the CCTNS and the digital forensics platforms contain large quantities of personal and confidential data, which are therefore vulnerable to cyber-attacks. The lack of adequate security procedures such as encryption and multiple authentication could lead to security gaps and unauthorised access to sensitive information, compromising the efficiency of the system. While the possibility of integrating digital forensics into the CCTNS has significant benefits for police and crime detection in India, the resulting barriers to such integration require continued budgetary allocations for infrastructure and staff training.

## VIII. LEGAL ASPECTS

The legal structure in place for digital forensics and criminal and CCTNS in India has undergone massive changes to meet the challenges of modern crime detection, while also addressing complex issues of privacy and data protection. Digital forensics, the process of identifying, preserving and analysing electronic evidence, is important for the investigation of cybercrime and other crimes in the digital world. Digital forensics falls under the Indian Evidence Act 1872, and in particular Article 65 B, which is responsible for the admissibility of electronic evidence. This section requires that certification of electronic evidence give priority to its integrity in the proceedings. Miscellaneous: in the case of the Anvar P.V. separate distinctiveness of the mandate. secretarial secretariat, secretariat of the deceased. secretarial secretariat of the deceased. The martyrdom of the princess (2014), the decision of the Supreme Court, which defined the certification requirement, reversed the previous interpretation and set a high standard for digital evidence. Other court cases: Manu Sharma vs State (New Delhi NCR) (2010), which demonstrated the criticality of digital evidence for the judicial process, and Unnikrishnan vs State (2011), which recognised digital images as a primary evidence and was in line with the provisions of Section 65B of the Directive.

Recent legislative reforms have further integrated digital forensics into the broader legal system in India. The old laws, which were in place during the colonial era, have been replaced by the Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Susraksha Sanhita (BNSS) laws, which were enacted in 2023, and which require the collection of evidence in criminal proceedings in the modern context. The aim is to improve the transparency of the process and its scientific character. Miscellaneous, the provisions of the BNSS, 180(3), 254, 265, 266 and 308 allow for the use of acoustic technology for witness testimony and for the integration of acoustic technology into legal proceedings.

The CCTNS, introduced by the NCRB under the National e-Government Plan, facilitates real-time exchange of information between police stations, drives information requests in investigations, analyses and support for citizen activities. It operates within the legal scope of the Information Technology Act 2000, which outlines the handling of electronic data and the involvement of law enforcement authorities. Indian authorities have a mandate to investigate cyber-crimes against Indian computer systems irrespective of where the crime was committed. As one of the initiatives of the Interoperable Criminal Justice System (ICJS), the CCTNS is linked to e-trial, e-prison, e-forensics and e-prosecution systems, in order to ensure a coherent approach to the delivery of justice.

The CCTNS also increases transparency through online services, including the tracking of FIRs and the reporting of complaints, which are available via the national citizens portals. However, the problem is that there is no comprehensive data protection law, which confuses the legal compliance of the Directive. The Personal Data Protection Bill, which has yet to be approved, leaves loopholes in the protection of the vast amount of personal data held by the CCTNS and creates a fear of abuse.

The CCTNS' large-scale collection of data, including sensitive personal and criminal records, poses serious privacy risks. The IT Act of 2000 provides few safeguards, mainly in the form of data security and lawful interception. However, without a strong data protection regime, unauthorised access or data breaches are possible, as is clear from the discussions on the Aadhar card case, where the bulk collection of data raised similar concerns. Experts say that to avoid such risks, the CCTNS must implement strict access controls and encryption.

The absence of a comprehensive data protection law exacerbates these problems. The proposed law on personal data protection should close

these loopholes, but until it is implemented, CCTNS operates in a legal grey area between the rights of law enforcement and the rights of individuals. Courts have highlighted the import of guarantees, particularly when CCTNS data are used as evidence, where compliance with Section 65B for authenticity is required.

Moreover, lack of resources in forensic laboratories and lack of staff trained in the detection of evidence is hindering the detection of effective evidence. There is little awareness of digital forensics among law enforcement and the public, which requires training programmes. The transnational nature of cybercrime also requires cooperation between countries, which is hampered by differences in legal standards.

In addition, it includes the adoption of a law on personal data protection to strengthen privacy protection legislation and investment in forensic infrastructure. Better partnerships between law enforcement and academia, and even with businesses, can foster innovation in digital forensics. Periodic changes in the legal structures will ensure that they are adapted to technological developments, while maintaining the balance between the provision of justice and the rights of individuals.

The laws governing digital forensics and CCTNS in India show a commitment to bring the criminal justice system in line with technology. BNS, BNSS and BSA together with the Indian Evidence Act provide a consolidated support for the use of digital evidence and the CCTNS enhances the investigative efficiency. However, the challenges of privacy issues and resource constraints are formidable. It will be important to address these elements through comprehensive legislation and capacity building in order to enable the system to achieve its potential.

## IX. IMPACT ON POLICING

The use of digital forensics and CCTNS has changed policing in India and it is being updated with modern technological advances. The digital forensics domain requires a scientific study of electronic evidence to support the investigation of cyber and traditional crimes with digital aspects. This report analyses how the use of technology has affected police work, examining its impact on investigations, teamwork between different organisations, data-driven strategies, public confidence and the problems associated with its use.

When digital forensics is involved, law enforcement can now obtain and study electronic information such as phone data, e-mails, and video surveillance images. This will allow cyber-crimes such as insider dealing and identity theft to be tackled alongside traditional crimes involving digital footprints. A good example is the case of Sushant Singh Rajput in 2020, where the WhatsApp messages and phone data helped the CBI in its investigation. To further improve this, the CCTNS compiles the criminal records in a centralised and digital system, which includes first information reports, investigation information and the items on the charge sheets. By 2020, 93 percent of police stations could integrate all FIRs into the CCTNS, significantly reducing manual work and making cases more efficient. The system allows investigators to easily access criminal records and fingerprints, which makes investigations faster and more accurate.

The CCTNS has enabled various police agencies to communicate with their stations, district offices, headquarters and the NCRB without difficulty. This integration allows data to be shared quickly and easily by investigators working with different states or countries. With CRI-MAC on the CCTNS, authorities at national level can quickly share information and help locate people with criminal records in other countries. In Himachal Pradesh, the adoption of the CCTNS significantly reduced the time taken to check passports (from 70 days to 24 hours) and allowed the police to find 85 percent of missing women and 95 percent of missing children (India Insight). The integration of the inter-operable criminal justice system improves coordination by linking data from the police with data from courts, prisons and forensic laboratories, which helps to ensure justice.

The CCTNS database enables police to detect trends in crime and spikes in certain locations. This may lead to a better use of resources and more disease prevention measures. For example, if analytics identify areas with a higher crime rate, police can plan patrols accordingly. The use of information from past crimes to predict future ones is recognised by many as possible, but it is still under development and testing. In addition, there are a number of databases such as NDSO that help police to monitor and follow up criminals, thus promoting public safety. Acquiring these skills is changing India's approach from treating crime after it occurs to treating it in advance.

CCTNS has put in place services that make things more transparent and more believable to citizens. Complaints or checking the progress of cases are now possible to report on the internet, which means that citizens do not have to visit police stations as often. People praised this new

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

approach, which enabled the public to interact more with police officers. When things are done by computer systems, the opportunities for corruption are reduced. In Himachal Pradesh, the services helped to build good relations between the police and the community and increase the trust in the police.

Digital forensics and CCTNS have helped in many ways, but they also face many challenges. Digital forensics requires special training and equipment, but many forensic laboratories in India lack the necessary resources. Checking encrypted or deleted data adds additional complexity to the investigative process. Although the CCTNS has seen many benefits, some areas are slower to be transformed because police officers are reluctant to use it and because more training is needed. As the CCTNS currently collects a large amount of personal data, there is a high risk of misuse and loss of data in the wrong hands. To tackle these challenges, we need to continue to invest in labour, technology, and regulatory change.

The link between digital forensics and CCTNS has transformed the Indian police force considerably by improving the way investigations are conducted, the way teams work together and the way decisions are made using data. Using such technologies promotes trust by providing services that are friendly to the public and clearly explain how they work. While some challenges remain, overall technology has greatly improved India's police force and enabled it to meet world standards. If the difficulties in implementing policies are constantly addressed, their positive impact will be greater.

## X. FUTURE TRENDS

Some modern technologies will influence the way digital forensics evolves in India. Automating tedious tasks, finding commonalities and anomalies in vast amounts of data, AI and ML will make investigations shorter and more accurate. As data is increasingly stored in the cloud, cloud forensics is more important than ever. New ways are being developed to deal with the challenges posed by rapidly changing data and international laws, and to ensure that evidence from blockchains is secure. As smart home technologies and wearables generate a lot of data, researchers will need to develop new techniques for analysing this data.

With fraud and money laundering in bitcoin increasing, blockchain forensic techniques will be widely used. To investigate this, it will be essential to have techniques to track transactions on the blockchain. Big data analytics will enable law enforcement to rapidly work through large sets of data and reveal links and similarities in large scale cyber investigations. Using these tools, investigators can avoid gathering and arranging evidence and instead focus on more sophisticated stages of analysis. New technologies such as virtual reality (VR) and augmented reality (AR) are being used to help train forensic experts and to provide more detailed views of crime scenes. Quantum computing, although still in its early stages, has the potential to solve great cryptographic problems and to make data analysis much faster, which could have a lasting impact on digital forensics. In the end, cyber deception approaches involving honeypots will be used in investigations to lure out the attackers and find out how they plan to live.

These global trends are of great importance to India, which is growing its digital economy and its number of cybercrime offences. However, India is facing some challenges, such as the lack of well-trained forensic specialists and the need for better training opportunities. The development of own forensic tools and technologies will be essential to address local problems and reduce reliance on other countries for solutions.

CCTNS is expected to change and improve significantly, starting with the recent success of linking all police stations in India. The main future trend is greater cooperation with other criminal justice systems, such as the CCTNS, e-trial, e-policing and e-prosecution. It aims to ensure that data is moved easily and without delay, thereby simplifying the process and enhancing the teamwork within the justice system. Similarly, information from the Arms Licence Information System (ALIS) and the National Cybercrime Reporting Portal (NCRP) are already on the ICJS platform and will be further interconnected.

The contribution of artificial intelligence and predictive analytics will significantly improve the performance of CCTNS. UNIFY is an early example of how machine learning can link missing persons and criminals. It is likely that more police forces will use trend forecasts to guide their allocation of resources and their operations. By adopting this training, police will be able to move from reactive to proactive strategies, in line with international guidance. Citizens can use digital services to report problems, track FIRs and request verification. The portal now includes missing persons search and vehicle NOC services, which shows the

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

government's continued commitment to new services.

The CCTNS can also include the collection of data from digital forensics laboratories and the use of IoT to monitor crime occurrences. CCTNS is scalable, allowing for continuous improvement at low cost, which promotes its sustainability. New laws are needed in the area of digital forensics, as Article 65B of the Indian Evidence Act 1872 requires digital evidence to fulfil certain requirements before it can be admitted to the court. Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Sanhita (BSS) have recently been introduced and both require the collection of evidence and recording of audio and video evidence in serious crimes. However, changes in legislation and procedures are still needed to deal with cybercrime and to streamline evidence collection.

According to the CCTNS, the absence of comprehensive data protection legislation is a major obstacle to combating piracy. Once the law on data protection is enacted, it could help to ensure the security of all data stored by CCTNS and reduce privacy concerns. Moreover, by opposing the Budapest Convention on grounds of drafting, India is showing that it wants to retain control of its own information at global level, which may lead to an increase in global cybercrime legislation, which may ultimately determine the CCTNS's approach to data sharing. There are insufficient qualified digital forensics experts, and more efforts are needed in terms of training programmes and equipment. Forensic laboratories are not supplied with sufficient resources and the construction of new advanced equipment requires considerable resources and expertise. It will be crucial for the CCTNS to promote uniformity of implementation in all countries, particularly in those with bottlenecks, such as in Assam. As the CCTNS collects a large amount of information, it needs to be protected and encrypted in a way that ensures that it is not misused.

But opportunities abound. Unemployment is rampant. Digital India and the National e-Government Plan (NEP) are providing increased support to digital forensics and CCTNS, which will help to introduce new technologies for broadband security and protection against satellite hacking. By joining forces, law enforcement, universities, and industry can help create homegrown technologies and reduce our need for foreign solutions. Public awareness campaigns can raise awareness of digital forensics and help people to participate in crime prevention.

The widespread use of artificial intelligence, cloud computing and IoT forensics promises to bring about major changes and improvements in the use of digital evidence in India. The use of more advanced security systems, artificial intelligence and additional services for the public will help the CCTNS to achieve a proactive and open police force. Yet addressing these trends means tackling problems such as unemployment, regulation, and privacy. By focusing on training, building the necessary infrastructure, and establishing robust data protection laws, India can ensure that its digital police meet world and local standards, while making the public more secure and ensuring that justice is done properly.

## XI. RECOMMENDATIONS

Transforming Digital Forensics as part of CCTNS needs a number of key changes in planning and operations. Building up key infrastructure at the ground level is key to achieving results. Police stations in some of India's rural and semi-urban areas do not have reliable internet, the needed computers, or ways to store large amounts of data. The government can help by giving top priority to upgrading these hospitals and working together with state governments. After that, training and capacity-building should become an established part of the institution. It is important for police officers to undergo constant training in digital forensics, aspects of cyber law, and how to handle evidence. Creating forensic training centers and setting up certification programs helps to develop specialists who are familiar with modern forensic devices and comply with the rules of the law.

Furthermore, established procedures and up-to-date guidance on the treatment of digital evidence at national level should be established. They should manage the process from the time of data collection to the time of storage in such a way that evidence can be presented in court without being altered. In addition, privacy and constitutional rights should be included in the rules and procedures of these agencies. Another important step is to enhance the security and data protection of CCTNS and forensic platforms. As more sensitive data is now collected and stored, strong encryption, multi-factor authentication and frequent audits are needed to ensure data security. In order to ensure the security of digital investigations,

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

legislation needs to be implemented alongside these platforms.

Besides, improving the way national databases, including NATGRID, NCRB, ICJS, and those of the courts create links, is necessary. Real-time sharing of information among departments allows for quicker detection and solve crimes. A number of regional digital forensic labs that use new devices and are run by skilled people will reduce reliance on a few national ones and will help process cases faster. Evaluating these reform's progress, remaining open to the public, and paying attention to public feedback should be part of monitoring them. Fulfilling these recommendations will make India's criminal justice system fitter, fairer, and ready to face crimes that take place on the Internet.

## XII. CONCLUSION

Overall, the use of digital forensics by the Criminal and Criminal Tracking Network and Systems (CCTNS) is changing the Indian criminal justice landscape considerably. The results show that when digital forensics works well with CCTNS, it increases the speed of detection and investigation, improves data accuracy and co-ordinates between agencies. It underlines that official rules and robust legal measures are needed to ensure that digital evidence is reliable and admissible in criminal investigations. The study shows that, while the CCTNS has improved the police system with technology and set up a national crime database, it can do more with the help of modern scientific equipment and top-level expertise. This shows that ensuring ethical and legal digital evidence requires both legislation, such as the Indian Evidence Act, and digital privacy legislation.

Research also identifies some major challenges in integrating HIMs- including the construction of new infrastructure, training of health professionals, data protection issues and interoperability of systems. Yet these problems can be addressed piecemeal, by improving legislation, providing additional training, and introducing cyber security measures. The study shows that a smooth and regulated integration of digital forensics and CCTNS will be of great help to India in its fight against cybercrime, organised crime and terrorism. Ultimately, it can open the door to a more open, efficient and modern justice system.