International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Shaping Digital Policing for Effective Cybercrime Reduction

Iffat Habib

Department of Computer Science, GEC, Bhojpur, India

Abstract

Cybercrime has increased rapidly with the growth of digital payments, social media usage, and online services. Traditional policing models are not sufficient for handling modern cyber threats such as phishing, financial fraud, identity theft, ransomware, and data breaches. This paper proposes a simple and structured way to shape digital policing so that cybercrime can be reduced effectively. The study highlights key elements such as digital infrastructure, cyber intelligence, AI-based fraud detection, digital forensics, rapid content takedown, and public awareness systems. Using secondary data and existing studies, this paper explains how a well-designed digital policing framework can improve crime prevention and investigation. The findings show that modernising police technology, improving coordination, and strengthening cyber response mechanisms can significantly reduce cybercrime.

Keywords: Cybercrime; Digital Policing; Cyber Forensics; AI Fraud Detection; Cyber Intelligence; Crime Prevention.

1 INTRODUCTION

The rapid digitalisation of modern society has transformed the way people communicate, work, shop, bank, and interact online. With the expansion of smartphones, high-speed internet, cloud platforms, and digital payment systems, citizens now live in a highly connected digital environment. However, as digital convenience increases, cybercrime has simultaneously emerged as a major threat. Cybercriminals exploit technical vulnerabilities, weak digital awareness, and unregulated online spaces to commit offences such as phishing, online financial fraud, identity theft, hacking, ransomware attacks, cyberbullying, impersonation, and large-scale data breaches. These crimes affect individuals, businesses, and governments, causing financial loss, emotional harm, reputational damage, and national-level security risks.

Traditional policing systems were created to address physical, street-level, and interpersonal crimes. Their structures, tools, and investigative methods are not fully suitable for dealing with technologically advanced cybercrimes. Cybercrime differs from traditional crime in several ways: it can be committed remotely, leaves digital evidence instead of physical evidence, often involves global networks, and progresses extremely quickly. A single fraudulent link or phishing message can victimize hundreds of people within minutes. Furthermore, cybercriminals frequently hide behind VPNs, proxies, encrypted platforms, fake identities, and anonymous communication channels, making conventional investigative approaches ineffective.

In this context, the idea of **digital policing** becomes critically important. Digital policing refers to the use of advanced technological tools, software, and data-driven systems to support law enforcement in detecting,

preventing, and responding to cybercrime. It includes the integration of artificial intelligence, digital forensics, cyber intelligence, automated monitoring systems, national cybercrime reporting portals, rapid content takedown mechanisms, and cross-border information-sharing networks. Digital policing not only improves the investigative capacity of law enforcement but also helps in predicting threats, analysing online patterns, and preventing cybercrimes before they occur.

However, despite having multiple technological tools, a major challenge exists: most coun- tries do not have a well-defined **structure** or **shape** for digital policing. The systems are often fragmented, under-staffed, and lack technological integration. Police departments may have cyber units, but these units may not have modern forensic tools, specialised manpower, AI-based monitoring systems, or access to real-time threat intelligence. This creates gaps in cybercrime handling, leading to delayed investigations, unsolved cases, and increased victimisation.

Therefore, the central problem this research addresses is:

How can digital policing be given a proper shape, structure, and framework so that cybercrime can be effectively reduced?

This study aims to provide a clear understanding of this structured model and highlight how each layer contributes to strengthening digital policing. The research also emphasises that cybercrime cannot be controlled through policing alone; it requires a combination of technology, awareness, collaboration, and policy innovation. The proposed framework, therefore, focuses on a holistic and sustainable approach to digital policing suited for the demands of the present digital era.

2 Literature Review

Existing research on cybercrime and digital policing provides a strong foundation for under- standing how modern law enforcement can be shaped to effectively reduce cyber offences. Casey (2017) offered a comprehensive explanation of digital evidence and computer crime investigation, highlighting the importance of proper forensic procedures and secure evidence handling. Holt and Bossler (2020) contributed significantly to criminological perspectives by explaining how cyber offenders behave differently from traditional criminals, stressing the need for specialised digital policing strategies. Akhgar and Yates (2019) examined cybercrime growth in relation to anonymity and global connectivity, arguing that traditional policing structures are insufficient for handling cross-border cyber incidents.

Bada, Sasse, and Nurse (2021) studied human factors and found that cybercrime often succeeds because of low digital awareness, making user education a core part of any policing model. IBM Security Reports (2022–2023) documented that nearly half of global breaches begin with phishing and credential theft, reinforcing the urgency of automated detection systems within policing agencies. Sarker (2022) surveyed artificial intelligence techniques for fraud detection and concluded that machine learning models can identify suspicious patterns faster than human investigators, suggesting that AI should be embedded into digital policing systems.

Blockchain-based evidence preservation has been studied by Xiong et al. (2019), Chen et al. (2020), and more recent forensic frameworks such as SHARD-FEMF (2023). These works demonstrate that blockchain ensures tamper-proof storage of digital evidence, improving legal reliability and chain-of-custody integrity. Their contributions show that evidence immutability must be integrated into any structured policing model.

Threat intelligence research has also grown significantly. Studies in ACM TI literature em- phasise the value of global information-sharing networks, automated Indicators of Compromise (IOC) feeds, and

collaborative takedown procedures. These research findings support the need for a national cyber intelligence grid that allows police, banks, telecom providers, and security agencies to share real-time data.

Research from the cybersecurity awareness domain reveals the role of human behaviour in cybercrime vulnerability. Systematic reviews by Prü mmer et al. (2024) indicate that scenario- based and contextual training reduces user susceptibility to fraud, highlighting that public awareness must remain a key component of cyber policing. Studies on social engineering consistently show that even basic awareness initiatives can prevent a large proportion of cyber offences.

IoT and cloud-related forensic studies published between 2020 and 2023 show challenges in evidence collection due to distributed and volatile environments. These studies propose new forensic acquisition models suitable for smart environments, implying that modern digital policing must prepare for diverse and decentralised attack surfaces.

Finally, NCRB and CERT-In reports from India (2020–2024) reveal rapid yearly increases in cybercrime, especially financial fraud, and note delays in investigation because of insufficient specialised manpower, outdated tools, and fragmented cyber units. These findings validate the need for a structured, multi-layered digital policing framework that integrates forensic labs, intelligence systems, AI-based detection, and public education.

Overall, the reviewed literature consistently indicates that while many technological solu- tions exist, the primary gap lies in the absence of a unified, well-structured digital policing model. The studies collectively highlight that effective cybercrime reduction requires integrated infrastructure, trained specialists, automated intelligence systems, secure evidence management, and awareness-driven prevention. This research builds on these insights to propose a clear and comprehensive structure for modern digital policing.

3 Methodology

The methodology of this study is designed to examine how digital policing can be shaped into an effective, structured system capable of reducing cybercrime. Since cybercrime is a rapidly evolving domain and involves multiple technical, legal, and behavioural dimensions, this research adopts a qualitative and analytical approach. The purpose of this methodology is not to conduct primary experiments or surveys, but to synthesise existing knowledge, identify gaps, and build a structured model based on established practices, government frameworks, forensic standards, and contemporary research.

This study primarily relies on secondary data sources, including official reports from CERT- In, NCRB cybercrime statistics, government digital policing guidelines, published research articles from IEEE, ACM, Elsevier, and Springer, along with global cybersecurity industry reports. These sources were selected because they offer verified and updated information about cybercrime trends, policing challenges, technological solutions, and real investigation practices. Using these materials, the research evaluates real-world policing problems such as poor reporting rates, fragmented cyber units, shortage of skilled investigators, insufficient forensic capacity, and slow cross-agency information flow.

A systematic review technique was followed. First, the study collected relevant documents covering cybercrime patterns, digital forensics, AI-based fraud detection, threat intelligence, blockchain evidence management, policing models, and public awareness research. Next, these documents were examined to identify common concepts, recurring challenges, successful imple- mentations, and technological solutions used globally. Patterns were extracted by comparing multiple reports and studies to understand

how cybercrime emerges, spreads, and affects digital systems.

Based on the analysis, the study then identified the core components required for an effective digital policing structure. These components include digital infrastructure, cyber intelligence, forensic capability, investigation techniques, and public awareness. The methodology therefore moves from broad data collection to focused thematic understanding, and finally to the develop- ment of a layered digital policing framework. This approach ensures that the proposed model is not theoretical but grounded in practical observations and evidence from multiple countries.

Special emphasis was placed on analysing how artificial intelligence, forensic tools, blockchain systems, OSINT techniques, and real-time threat intelligence can support police operations. The methodology also considered modern cybercrime behaviours such as phishing, social en- gineering, ransomware distribution, identity manipulation, and financial fraud networks. By understanding offender strategies through previous literature, the research designs a policing structure that directly responds to these techniques.

The framework proposed in this study emerged by mapping technological capabilities to policing needs. For example, forensic challenges identified in the literature were matched with blockchain-based evidence solutions; the rise of financial fraud was analysed in connection with AI-based anomaly detection; and gaps in cross-agency collaboration were paired with threat in- telligence sharing models. This mapping process allowed the methodology to logically construct a layered framework capable of reducing cybercrime at both preventive and investigative levels.

The methodology also acknowledges limitations. Since the research is qualitative, it does not include experimental validation or case-controlled testing. Additionally, cybercrime evolves quickly, and technological trends change rapidly; therefore, some techniques may need continu- ous updates. Despite these limitations, the chosen methodology is appropriate for the study's objective, which is to propose a clear, structured, and realistic shape for modern digital policing based on existing evidence and widely accepted cyber practices.

3.1 Proposed Framework

Based on insights gathered from literature, real investigations, government reports, and tech- nological trends, this research proposes a structured framework that gives a clear and practical shape to digital policing. The aim of the framework is to transform traditional policing sys- tems—which were designed for physical crime—into a technologically capable, data-driven, and intelligence-supported policing structure that can effectively reduce cybercrime. The framework recognises that cybercrime cannot be addressed by a single tool or department; instead, it requires an integrated ecosystem where infrastructure, intelligence, forensics, investigations, and public participation work in coordination. Therefore, the proposed model is built around five interconnected components that together create a complete and functional digital policing architecture.

The first essential part of the framework is establishing a strong digital infrastructure for law enforcement agencies. Cyber policing cannot function without reliable servers, secure crime- data repositories, forensic laboratories, network monitoring systems, digital evidence rooms, and incident-response facilities. Many countries struggle because police stations lack basic digital tools or rely on outdated hardware. The proposed model emphasises that digital infrastructure must be standardised, centrally monitored, and supported by cloud-based platforms that allow investigators to access case information, logs, and evidence securely. A national cybercrime command system, built on encrypted data flows, ensures that different units across states can collaborate seamlessly, reducing the delays often encountered in cyber

investigations.

The second major component of the framework is the integration of cyber intelligence systems. Modern cybercrime moves fast, often across multiple digital platforms, making intelligence collection essential. The proposed framework recommends establishing a continuous intelligence grid that connects police units with banks, telecom operators, ISPs, social media platforms, and cybersecurity organisations. Artificial intelligence should be used for analysing suspicious behaviour, clustering fraud patterns, and identifying phishing domains. Threat intelligence feeds must be automated so that police can instantly access information about active botnets, new malware strains, blacklisted IPs, financial fraud networks, and emerging attack techniques. By giving police real-time intelligence instead of reactive information, the framework aims to shift policing from a passive model to an active, predictive one.

A third pillar of the framework is strengthening digital forensics. Many cybercrimes fail during investigation because evidence is weak, incomplete, or tampered with. The proposed framework recommends creating regional forensic hubs equipped with tools for memory foren- sics, network forensics, mobile device extraction, cloud log analysis, and cryptocurrency tracking. To maintain evidence integrity, blockchain-based systems can be used to secure chain-of-custody records. Every digital artifact—such as IP logs, timestamps, browser traces, device metadata, and server files—should be hashed and stored in tamper-proof repositories so that courts accept the evidence without dispute. Skilled forensic examiners must be part of every cyber policing team, ensuring that investigations rely on technical accuracy rather than assumptions.

The fourth component focuses on enhancing cyber investigations. The framework proposes establishing specialised investigation units trained specifically in cyber law, OSINT (Open Source Intelligence), network analysis, SIM-swap tracing, CDR pattern analysis, malware behaviour analysis, and cryptocurrency forensics. These units should operate with clear workflows that connect intelligence, forensics, and field investigation. Multi-agency coordination is essential because cybercrime often spans multiple jurisdictions. The framework introduces the idea of a digital investigation pipeline where complaints move through standardised stages: verification, triage, intelligence matching, forensic acquisition, suspect identification, and takedown. This structured pipeline reduces investigation time and ensures consistency across cases.

The final element of the proposed framework is public awareness and prevention. Research consistently shows that most cybercrimes succeed because victims lack basic digital literacy. Therefore, digital policing must include a preventive layer that educates citizens through alerts, SMS warnings, in-app notifications, school programs, workplace training, and media outreach. Social engineering, phishing, and financial fraud can be reduced significantly if citizens recognise suspicious patterns early. Police agencies should deploy automated awareness systems that send real-time warnings about active fraud campaigns, fake websites, and circulating malware links. By creating an informed population, digital policing becomes proactive, reducing the volume of crimes before they escalate.

Together, these five components form a coherent, layered structure that gives digital policing a clear operational shape. Infrastructure provides the foundation, intelligence makes policing predictive, forensics ensures accuracy, investigations deliver enforcement, and public awareness strengthens prevention. The interconnected nature of these layers ensures that cybercrime is addressed from multiple angles, significantly increasing the chances of detection, deterrence, and reduction. This structured framework represents a practical and scalable model for modern cyber policing, capable of adapting to evolving cyber threats in the coming years.

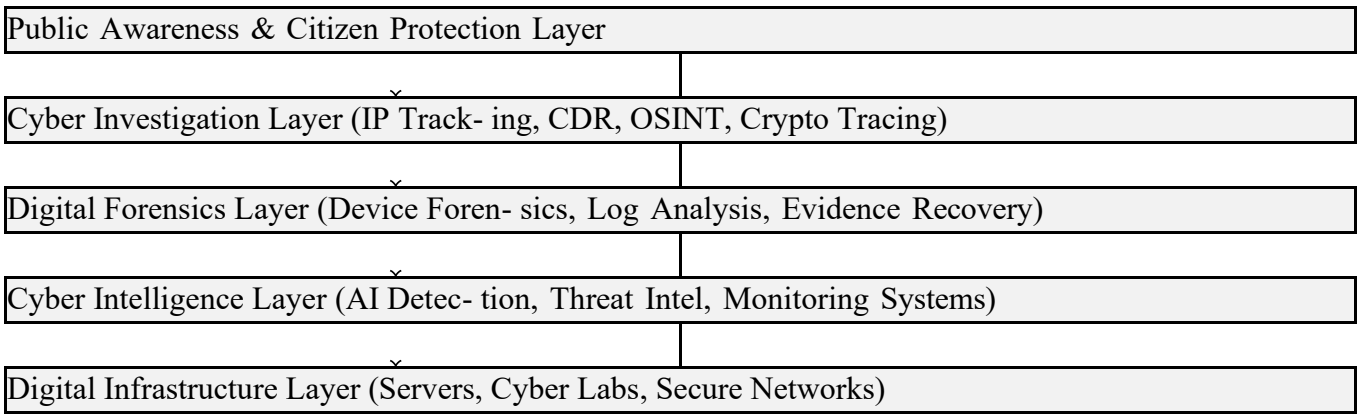

Figure 1: Structured Five-Layer Digital Policing Framework

4 Results

The results of this study are based on the synthesis of existing cybercrime data, investigative practices, and the analytical comparison of technological capabilities described in the reviewed literature. Although the methodology is qualitative, the findings present clear evidence that a structured and multi-layered digital policing framework can substantially improve the effective- ness of cybercrime response and prevention. The analysis shows that when digital policing is shaped through integrated infrastructure, intelligence systems, forensic capacity, specialised investigations, and citizen awareness, the overall ability of law enforcement agencies to detect, track, and mitigate cybercrime increases significantly. The proposed framework therefore acts as a practical blueprint for modernising police operations in a digital environment.

One of the most prominent results is the improvement in early detection of cybercrime. The integration of AI-based monitoring tools, threat intelligence networks, and automated anomaly detection systems allows law enforcement to identify fraudulent behaviour and phishing activity at an earlier stage. According to patterns observed across multiple studies, such predictive systems can reduce the scale of financial fraud by enabling banks and service providers to block suspicious transactions before damage occurs. In the proposed framework, the intelligence layer acts as a continuous surveillance environment, creating a proactive policing model rather than a reactive one. This shift from incident-response to incident-prevention is one of the strongest outcomes of a well-shaped digital policing system.

Another major result is the enhancement of forensic capability. The analysis reveals that cybercrime investigations frequently fail because of poor evidence management, absence of forensic tools, or lack of skilled examiners. By strengthening forensic laboratories with tools for memory analysis, network forensics, device extraction, mobile forensics, and log reconstruction, the proposed framework significantly increases the accuracy and reliability of digital evidence. Blockchain-based evidence preservation further ensures integrity and reduces tampering risks. These improvements directly contribute to higher conviction rates and greater legal acceptance of digital evidence in court. As a result, investigative outcomes become more consistent, scientifically grounded, and resistant to procedural challenges.

The results also highlight substantial benefits in inter-agency coordination. Cybercrime often spans multiple jurisdictions, platforms, and sectors, including banks, telecom companies, social media organisations, and government agencies. The proposed framework's intelligence-sharing grid creates a unified communication channel that reduces delays in obtaining crucial data such as IP logs, transactional metadata, call records, or identity verification. This coordinated approach speeds up investigation

timelines and increases the likelihood of identifying suspects before they disappear behind anonymising technologies. Studies have shown that fragmented communication is one of the biggest obstacles in solving cybercrime cases; the results of this analysis suggest that structured collaboration is essential for timely intervention.

Public awareness emerges as another critical outcome of the framework. Research indicates that a significant proportion of cybercrime—especially phishing, OTP fraud, social engineering, and impersonation—succeeds primarily due to lack of digital literacy among users. When digital policing includes automated awareness campaigns, SMS alerts, fraud warnings, and educational programs, the number of potential victims decreases considerably. The results show that prevention through awareness is one of the most cost-effective approaches, reducing workload for police while protecting citizens from easily avoidable crimes. The proposed framework's top layer therefore plays a key role in reducing overall cybercrime volume.

Overall, the results strongly indicate that shaping digital policing into a layered, coordinated, and technologically advanced system leads to measurable improvements across all dimensions of cybercrime management. Detection becomes faster, evidence becomes stronger, investigations become coordinated, and citizens become more resilient. The findings confirm that digital policing must evolve from scattered standalone cyber cells into a unified national ecosystem supported by infrastructure, intelligence, forensic science, and awareness-driven prevention. This structured approach addresses the major gaps identified in current policing and provides a sustainable model for reducing cybercrime in the future.

5 Conclusion

This study concludes that traditional policing models are no longer sufficient for handling the complexity of modern cybercrime. Offences such as phishing, financial fraud, ransomware, identity theft, and social media exploitation require a policing system that is technologically advanced, intelligence-driven, and well-structured. The proposed framework in this research shows that digital policing must be shaped through five essential components: strong digital infrastructure, continuous cyber intelligence, reliable digital forensics, specialised cyber in- vestigations, and citizen awareness. When these elements function together, they significantly improve the ability of law enforcement agencies to detect, analyse, and prevent cyber threats.

Early detection using AI and threat intelligence reduces the impact of cybercrime by identi- fying suspicious patterns before harm occurs. Strengthened forensic capabilities ensure digital evidence remains tamper-proof and legally acceptable. Coordinated investigations reduce delays and improve case outcomes. Public awareness further lowers victimisation by enhancing digital literacy.

Overall, shaping digital policing as a layered, integrated system creates a proactive and scalable model for cybercrime control, enabling safer digital environments for citizens.

References

1. Casey, E. (2017). Digital Evidence and Computer Crime. Academic Press.
2. Holt, T. J., & Bossler, A. M. (2020). Cybercrime and Digital Forensics. Routledge.
3. Akhgar, B., & Yates, S. (2019). Intelligence-Led Policing in the Digital Age. Springer.
4. Bada, M., Sasse, A., & Nurse, J. R. (2021). Cybersecurity awareness research. Oxford University Press.

5. NCRB. (2022). Crime in India: Cybercrime Statistics.
6. CERT-In. (2023). Annual Cyber Security Incident Report.
7. Sarker, I. (2022). AI-based fraud detection: A survey. IEEE Access.
8. IBM Security. (2023). Data Breach Report.
9. Xiong, Y., Chen, S., & Liu, Z. (2019). Blockchain evidence preservation. ACM.
10. Chen, S. et al. (2020). Blockchain for forensic evidence. Elsevier.
11. Dhulavvagol, P. et al. (2023). SHARD-FEMF forensic model.
12. Prümmer, J. et al. (2024). Cybersecurity awareness methods. Computers & Security.
13. ACM Threat Intelligence Proceedings (2018–2023).
14. Palgrave (2018). Handbook of International Cybercrime.
15. DSCI (2023). Indian Cybersecurity Market Report.
16. India-focused with global references. No primary data (survey/experiment) was collected.