UGC & Govt. Approved
Sonargaon University (SU)
সোনারগাঁও ইউনিভার্সিটি (এসইউ)

RESEARCH MONOGRAPHY
on
ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE IN CRIMINAL TRIALS: CHALLENGES IN THE MODERN CRIMINAL PROCEDURE SYSTEM

Supervised by:

Sunzida Akhter

Lecturer

Department of Law

SONARGAON UNIVERSITY(SU), Dhaka

Submitted by:
Atanu Roy
ID-LLB2203027020

BATCH-27TH

Department of Law

SONARGAON UNIVERSITY(SU), Dhaka

Date of Submission : 25th June, 2026

Acknowledgement

First and foremost, I express my sincere gratitude to Almighty God for providing strength, patience, and guidance throughout the completion of this thesis.

I would like to express my deepest appreciation to the faculty members of the Department of Law, Sonargaon University, for their academic support and encouragement during my LLB programme.

I extend special thanks to my respected thesis supervisor for valuable guidance, constructive suggestions, and continuous encouragement throughout the preparation of this research work.

I am also grateful to my teachers, friends, and classmates whose support and academic discussions contributed to the development of this study.

Finally, I express heartfelt gratitude to my family for their patience, encouragement, and continuous support throughout my academic journey.

Signature:

CERTIFICATION

This is to certify that the thesis entitled:

"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"

submitted by **Atanu Roy**, Department of Law, Sonargaon University, in partial fulfilment of the requirements for the degree of **Bachelor of Laws (LLB)**, is a record of original academic work carried out under my supervision and guidance.

To the best of my knowledge and belief, this thesis has not previously been submitted, either in whole or in part, to any other university or institution for the award of any degree, diploma, or academic qualification.

I further certify that the work presented in this thesis is satisfactory in scope and quality for submission and evaluation under the academic requirements of Sonargaon University.

……..

Sunzida Akhter

Lecturer

Department of Law

Sonargaon University

DECLARATION

I hereby declare that the thesis entitled:

"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"

submitted to the Department of Law, Sonargaon University, in partial fulfilment of the requirements for the degree of **Bachelor of Laws (LLB)**, is my own original work and has been completed under academic supervision.

I further declare that this thesis has not been submitted previously, either wholly or partly, to any other university, institution, or authority for the award of any degree, diploma, or academic qualification.

All information, ideas, and materials obtained from published and unpublished sources have been properly acknowledged and referenced in accordance with the **APA referencing style**.

I accept full responsibility for the authenticity and academic integrity of this research work.

Submitted by:

Name: **Atanu Roy**
Student ID: **LLB2203027020**
Programme: **Bachelor of Laws (LLB)**
Department: **Law**
University: **Sonargaon University**

LETTER OF TRANSMITTAL

To
The Supervisor
Department of Law
Sonargaon University

Subject: Submission of Thesis Report titled"Admissibility and Reliability of Digital Evidence in Criminal Trials: Challenges in the Modern Criminal Procedure System"

Respected Madam,

With due respect, I would like to submit my thesis .This thesis has been prepared and submitted as partial fulfilment of the requirements for the degree of **Bachelor of Laws (LLB)** under the Department of Law, Sonargaon University.I have completed this research work sincerely and carefully by following academic guidelines and maintaining the required standards of research and APA referencing style.I would like to express my gratitude for your valuable guidance, supervision, and support throughout the preparation of this thesis.

Therefore, I respectfully request you to accept this thesis and consider it for evaluation.

Yours faithfully,

Atanu Roy
Student ID: **LLB2203027020**
Programme: **Bachelor of Laws (LLB)**
Department of Law
Sonargaon University

TABLE OF CONTENTS

ABSTRACT

Digital evidence has become an increasingly important component of criminal investigation and judicial decision-making in modern criminal justice systems. The rapid development of information technology, electronic communication, digital devices, and internet-based platforms has transformed both criminal activity and evidentiary practices. As a result, courts increasingly rely on electronic records, digital communications, surveillance data, and forensic findings during criminal trials.

This research examines the admissibility and reliability of digital evidence in criminal trials and analyses the challenges faced by modern criminal procedure systems in regulating electronic information. The study explores the legal principles governing admissibility, including relevance, authenticity, integrity, legality of collection, and procedural fairness. It further investigates factors influencing reliability such as manipulation, technical error, forensic limitations, chain of custody, and evidentiary preservation.

The research adopts a qualitative doctrinal legal research methodology based on analysis of legal principles, academic literature, procedural standards, and scholarly discussion. Both primary and secondary legal sources were considered in developing the analysis.

The findings indicate that digital evidence provides significant benefits for criminal justice administration but also introduces complex legal and procedural concerns. Reliability depends not only on technological capability but also on effective authentication procedures, proper forensic examination, judicial oversight, and protection of procedural rights.

The study concludes that criminal procedure systems should strengthen evidentiary standards, improve institutional capacity, and adapt legal frameworks to technological development in order to maintain fairness and public confidence in judicial outcomes.

Keywords: Digital Evidence, Criminal Trial, Admissibility, Reliability, Criminal Procedure, Electronic Evidenc

Chapter One: Introduction

1.1 Background of the Study

The advancement of digital technology has transformed modern society and substantially influenced criminal justice systems across the world. The increasing use of computers, smartphones, electronic communication, cloud storage, social networking platforms, surveillance technologies, and internet-based services has changed both the nature of criminal activity and methods of criminal investigation. As a result, digital information has become one of the most significant sources of evidence in contemporary criminal trials.

Digital evidence refers to information of probative value that is stored, transmitted, or generated in digital form and may be presented before a court to establish facts in dispute. Common examples include emails, text messages, call records, CCTV footage, social media communications, electronic documents, metadata, GPS records, website activity logs, and information extracted from mobile devices or computer systems.

In criminal proceedings, digital evidence performs an increasingly important role in identifying offenders, reconstructing events, supporting witness testimony, and establishing guilt or innocence. Law enforcement agencies now rely heavily on forensic technology and electronic investigation methods to detect and prosecute offences including cybercrime, financial fraud, terrorism, organised crime, and conventional offences involving electronic communication.

Despite its growing importance, the use of digital evidence raises complex legal and procedural concerns. Traditional evidence law was developed primarily for physical and documentary evidence and may not fully address the characteristics of electronic data. Unlike physical evidence, digital evidence can be copied, modified, deleted, manipulated, encrypted, or transferred rapidly without visible alteration. Consequently, courts often face difficulties in determining whether digital materials should be admitted and whether they can be considered trustworthy.

The admissibility of digital evidence concerns the legal standards that govern whether electronic information may be accepted by a court as evidence. Courts generally require proof that digital evidence is relevant, authentic, legally obtained, and properly preserved.

Reliability refers to the degree to which digital evidence accurately represents the facts and remains free from corruption, tampering, or technical error.

Modern criminal procedure systems therefore face an important challenge: ensuring that technological innovation supports justice without compromising procedural fairness and legal certainty. Questions relating to authentication, chain of custody, privacy protection, forensic examination, and evidentiary integrity have become central issues in contemporary criminal litigation.

This research examines the admissibility and reliability of digital evidence in criminal trials and analyses the challenges that emerge within modern criminal procedure systems. The study further seeks to explore legal approaches and identify measures that may strengthen evidentiary standards and improve the administration of criminal justice.

1.2 Statement of the Problem

The increasing dependence on digital technology in modern society has significantly expanded the use of digital evidence in criminal investigations and criminal trials. Electronic communications, mobile devices, surveillance systems, online records, and computer-generated information are now frequently presented before courts as evidence. Although digital evidence has strengthened investigative capacity and improved access to information, its widespread use has also created serious legal and procedural challenges.

One of the major problems concerns the admissibility of digital evidence. Traditional rules of evidence were largely designed for physical documents and tangible materials and often provide limited guidance for handling electronic information. Courts frequently face uncertainty in determining whether digital evidence satisfies legal requirements relating to authenticity, relevance, legality of collection, and evidentiary integrity.

Another important issue concerns reliability. Digital information possesses characteristics that distinguish it from conventional evidence. Electronic data may be altered, duplicated, deleted, manipulated, encrypted, or accessed remotely without immediate detection. Such vulnerabilities raise concerns regarding whether digital evidence accurately reflects the original facts and whether it can be trusted during judicial decision-making.

The process of collecting and preserving digital evidence also presents practical difficulties. Weak chain-of-custody procedures, technical limitations, inadequate forensic expertise, improper storage systems, and procedural irregularities may reduce evidentiary value and create risks of wrongful judicial outcomes. Courts must therefore determine not only whether digital evidence exists but also whether it has remained authentic and reliable throughout the investigative process.

Furthermore, technological development often progresses more rapidly than legislative reform. In many jurisdictions, criminal procedure laws continue to evolve in response to emerging technologies, creating gaps between legal standards and investigative practice. These gaps may generate inconsistency in judicial decisions and uncertainty in evidentiary assessment.

Accordingly, there is a growing need to examine the legal standards governing admissibility and reliability of digital evidence and to identify challenges faced by modern criminal procedure systems. This research seeks to address these concerns by evaluating existing legal approaches and proposing measures to strengthen procedural safeguards and promote fair administration of criminal justice.

1.3 Research Objectives

The primary objective of this study is to examine the admissibility and reliability of digital evidence in criminal trials and analyse the challenges arising within modern criminal procedure systems due to technological advancement.

The specific objectives of the study are:

1. To examine the concept, nature, and legal significance of digital evidence in criminal proceedings.
2. To analyse the legal principles governing admissibility of digital evidence, including relevance, authenticity, integrity, and legality of collection.
3. To identify the major challenges affecting reliability of digital evidence, including manipulation, alteration, technical error, and evidentiary preservation.
4. To evaluate the importance of authentication procedures, chain of custody, and forensic examination in maintaining evidentiary trustworthiness.
5. To examine the relationship between digital investigation practices and principles of procedural fairness, privacy, and human rights.

6. To assess the effectiveness of modern criminal procedure systems in addressing evidentiary issues created by digital technologies.
7. To provide recommendations for improving legal frameworks and institutional practices concerning digital evidence in criminal trials.

Through achieving these objectives, the study aims to contribute to a better understanding of how criminal justice systems may ensure both admissibility and reliability of digital evidence while preserving fairness and legal accountability.

1.4 Research Questions

This research is guided by a number of questions that aim to examine the legal and practical challenges surrounding the admissibility and reliability of digital evidence in criminal trials. These questions provide the analytical framework for the study and assist in achieving the research objectives.

The study seeks to answer the following questions:

1. What is digital evidence and what are its major characteristics in criminal proceedings?
2. What legal principles determine the admissibility of digital evidence in criminal trials?
3. What factors influence the reliability and authenticity of digital evidence?
4. What challenges arise during the collection, preservation, examination, and presentation of digital evidence?
5. How do issues such as alteration, manipulation, technical error, and chain of custody affect evidentiary reliability?
6. To what extent do existing criminal procedure systems adequately regulate the use of digital evidence?
7. What reforms or procedural improvements can strengthen the admissibility and reliability of digital evidence in modern criminal justice systems?

These research questions will guide the discussion throughout the thesis and provide the foundation for legal analysis, evaluation of existing practices, and formulation of recommendations.

1.5 Significance of the Study

This study is significant because it addresses one of the most important emerging issues in contemporary criminal justice: the increasing dependence on digital evidence and the legal challenges associated with its admissibility and reliability. As technology continues to shape criminal activities and investigative methods, courts and legal institutions must adapt evidentiary rules to ensure fairness, accuracy, and effective justice.

The research contributes to academic understanding by examining the legal principles governing digital evidence and evaluating how modern criminal procedure systems respond to technological developments. It expands existing legal discussion by focusing not only on admissibility requirements but also on concerns relating to reliability, authenticity, and procedural integrity.

The study is also important for judicial practice. Judges frequently encounter electronic records, digital communications, surveillance materials, and forensic reports during criminal trials. A clearer understanding of evidentiary standards may assist courts in making consistent and legally sound decisions regarding the acceptance and evaluation of digital evidence.

For legal practitioners, including prosecutors and defence lawyers, the study provides insight into evidentiary requirements, procedural safeguards, and common challenges that arise when presenting or challenging digital evidence in criminal proceedings. Understanding these issues may improve advocacy and promote fair trial standards.

The research may further assist investigators and law enforcement agencies by highlighting the importance of proper collection, preservation, documentation, and forensic examination of electronic information. Effective handling of digital evidence can reduce risks of evidentiary exclusion and increase confidence in criminal investigations.

From a policy perspective, the findings of this study may support future legal reform by identifying limitations in current procedural frameworks and recommending measures to strengthen evidentiary regulation in response to technological advancement.

Finally, this research may serve as a useful academic resource for future researchers, students, and scholars interested in criminal law, evidence law, digital forensics, and the relationship between technology and justice.

1.6 Scope and Limitations of the Study

This study focuses on examining the admissibility and reliability of digital evidence in criminal trials within the context of modern criminal procedure systems. The research explores the legal principles governing the acceptance of electronic evidence and evaluates practical challenges associated with its collection, preservation, authentication, and presentation before courts.

The scope of this research includes an examination of the concept and characteristics of digital evidence and its growing importance in criminal justice administration. The study discusses common forms of digital evidence such as electronic documents, emails, mobile communications, digital photographs, surveillance recordings, metadata, internet records, and information obtained through electronic devices and digital forensic processes.

The research also analyses the evidentiary standards generally applied to determine admissibility, including relevance, authenticity, integrity, legality of acquisition, and procedural compliance. In addition, the study investigates factors influencing reliability, including risks of alteration, technical error, cyber manipulation, improper handling, and weaknesses in maintaining chain of custody.

This thesis primarily adopts a legal and doctrinal approach. It focuses on criminal procedure and evidence law rather than detailed technical or engineering analysis of digital forensic tools. Although references to technological processes may be included where necessary, the primary emphasis remains on legal evaluation and procedural implications.

Certain limitations should be recognised. Due to limitations of time, available resources, and the broad nature of technological development, the research does not attempt to examine every jurisdiction or all categories of digital evidence. Instead, it concentrates on broader legal principles and selected examples relevant to contemporary criminal justice systems.

Additionally, because digital technology evolves rapidly, legal standards and judicial approaches may continue to develop after completion of this study. Therefore, findings and recommendations should be understood within the context of ongoing legal and technological change.

Despite these limitations, the study aims to provide a comprehensive legal analysis and contribute to understanding the challenges and future development of digital evidence in criminal trials.

1.7 Research Methodology

Research methodology refers to the systematic approach adopted to collect, analyse, and interpret information for achieving the objectives of a study. Since this thesis examines legal principles and procedural challenges relating to digital evidence in criminal trials, a doctrinal and qualitative research methodology has been adopted.

This study primarily follows a doctrinal legal research approach. Doctrinal research focuses on identifying, analysing, and interpreting existing legal rules, judicial principles, and legal literature. Through this method, the research evaluates how laws governing criminal procedure and evidence regulate the admissibility and reliability of digital evidence.

The study relies mainly on qualitative analysis rather than statistical measurement. Qualitative legal research allows detailed examination of legal concepts, judicial reasoning, procedural standards, and academic interpretations relevant to digital evidence.

To achieve the objectives of the study, both primary and secondary sources of data are used.

Primary sources include:
- Constitutional provisions relevant to criminal justice and fair trial principles;
- Statutes and legislation relating to evidence law and criminal procedure;
- Judicial decisions and case law concerning electronic and digital evidence;
- Rules and legal guidelines applicable to evidentiary procedures.

Secondary sources include:
• Academic books and legal textbooks;
• Peer-reviewed journal articles;
• Research papers and scholarly publications;
• Government reports and policy documents;
• Legal commentaries and relevant academic materials.

The method of analysis adopted in this research is analytical and descriptive. The analytical method is used to critically evaluate legal rules and procedural practices, while the descriptive method explains concepts, legal developments, and practical challenges associated with digital evidence.

Where appropriate, the study may also apply limited comparative analysis to observe how different legal approaches address admissibility and reliability concerns in criminal proceedings.

The findings of this research are developed through interpretation and critical evaluation of legal materials rather than empirical field investigation. This methodological approach supports a structured examination of digital evidence and enables the formulation of practical recommendations for strengthening modern criminal procedure systems.

1.8 Chapter Organisation

This thesis is organised into five chapters in order to provide a systematic and logical examination of the admissibility and reliability of digital evidence in criminal trials and the challenges faced by modern criminal procedure systems.

Chapter One: Introduction

This chapter introduces the research topic and establishes the foundation of the study. It presents the background of the study, statement of the problem, research objectives, research questions, significance of the study, scope and limitations, research methodology, and overall structure of the thesis.

Chapter Two: Conceptual Framework and Literature Review

2.1 Concept and Meaning of Digital Evidence

The increasing use of digital technology in modern society has transformed the methods through which information is created, stored, communicated, and preserved. This transformation has also influenced criminal investigations and judicial processes, leading to the emergence of digital evidence as a significant category of evidence in criminal proceedings.

Digital evidence generally refers to information with evidentiary value that exists in electronic form and can be collected, preserved, examined, and presented before a court for determining facts relevant to a legal dispute. Unlike traditional evidence, which often exists in physical form, digital evidence is generated, processed, and maintained through electronic systems and technological devices.

Digital evidence may originate from various sources including computers, smartphones, servers, cloud storage systems, surveillance cameras, social media platforms, emails, websites, digital documents, mobile applications, internet records, GPS systems, and communication networks. These electronic records frequently play an important role in identifying suspects, reconstructing criminal events, verifying testimony, and establishing legal responsibility.

A distinguishing feature of digital evidence is that it is intangible in nature. Although the data may be stored in physical devices, the information itself exists electronically and can often be copied or transferred without changing its visible appearance. This characteristic creates both advantages and challenges within criminal justice systems.

Digital evidence differs from traditional evidence in several respects. First, it may be highly fragile because electronic data can be altered, deleted, corrupted, or manipulated. Second, digital information may be duplicated rapidly and distributed across multiple systems simultaneously. Third, access to digital evidence frequently requires specialised forensic techniques and technical expertise.

From a legal perspective, digital evidence is evaluated according to evidentiary principles similar to those applied to traditional evidence. Courts generally assess whether digital materials are relevant, authentic, reliable, and obtained through lawful procedures. However, because electronic information may be vulnerable to modification and technical interference, additional safeguards are often necessary to establish trustworthiness.

Digital evidence has become increasingly important in contemporary criminal trials because many modern crimes involve electronic communication or generate digital traces. Even conventional crimes such as theft, fraud, assault, or homicide may involve mobile records, surveillance footage, online interactions, or location data.

The growing dependence on digital information has encouraged legal scholars and judicial institutions to reconsider traditional evidentiary doctrines and adapt criminal procedure systems to technological realities. As a result, understanding the concept and legal nature of digital evidence has become essential for ensuring effective and fair administration of justice.

This chapter therefore establishes the conceptual foundation necessary for analysing later discussions concerning admissibility, reliability, and procedural challenges associated with digital evidence in criminal trials.

2.2 Characteristics and Types of Digital Evidence

Digital evidence possesses unique features that distinguish it from traditional forms of evidence. These characteristics influence how evidence is collected, preserved, examined, and evaluated during criminal proceedings. Understanding these characteristics is important because they directly affect issues of admissibility and reliability in modern criminal justice systems.

2.2.1 Characteristics of Digital Evidence

a. Intangible Nature

One of the primary characteristics of digital evidence is its intangible nature. Unlike physical evidence, digital information exists in electronic form and cannot be observed directly without technological devices or software. Although stored within physical hardware, the evidentiary value lies in the electronic data itself.

b. Fragility and Vulnerability

Digital evidence is highly sensitive to alteration, corruption, deletion, or accidental modification. A simple interaction with an electronic device may change metadata or system records. This vulnerability creates challenges in maintaining evidentiary integrity during investigation and trial.

c. Reproducibility

Digital data may be copied repeatedly without noticeable changes to appearance or content. While this allows efficient preservation and examination, it also increases the risk of unauthorised duplication and questions regarding authenticity.

d. Dependence on Technology

Access to digital evidence often requires specialised software, forensic tools, technical knowledge, and compatible hardware systems. Investigators and courts may depend on experts to interpret and verify electronic information.

e. Large Storage Capacity

Electronic devices can store significant amounts of information over long periods. As a result, investigators may collect extensive quantities of evidence that require careful filtering and analysis.

f. Hidden and Recoverable Nature

Even deleted digital information may sometimes be recovered through forensic techniques. This feature increases investigative opportunities but also raises concerns regarding privacy and procedural fairness.

g. Time and Metadata Sensitivity

Digital evidence frequently includes metadata such as timestamps, location information, system activity records, and user interactions. These details may provide important context during criminal investigations.

2.2.2 Types of Digital Evidence

Digital evidence appears in multiple forms depending on the technological environment and investigative circumstances.

a. Computer-Based Evidence

This category includes files stored in desktops, laptops, hard drives, external storage devices, system logs, browsing records, and electronic documents.

b. Mobile Device Evidence

Mobile phones and tablets generate extensive digital records including messages, call history, photographs, videos, application data, and location information.

c. Internet and Network Evidence

Internet activity often produces evidence such as browsing history, website records, online transactions, server logs, cloud storage information, and communication records.

d. Electronic Communication Evidence

This includes emails, text messages, instant messaging conversations, social media interactions, and other forms of electronic communication.

e. Audio and Video Evidence

Digital recordings obtained from surveillance systems, body cameras, CCTV footage, and electronic media frequently serve as evidence in criminal trials.

f. Metadata

Metadata refers to information about electronic data, including creation dates, modification records, file ownership, and usage history. Metadata often assists in verifying authenticity.

g. Cloud-Based Evidence

Cloud computing systems store information remotely rather than locally. Evidence from cloud services may present jurisdictional and procedural challenges during investigations.

The wide variety of digital evidence demonstrates its growing importance within criminal justice systems. However, these characteristics also create difficulties concerning preservation, authentication, and judicial evaluation, which directly influence admissibility and reliability in criminal trials.

2.3 Development of Digital Technology and Criminal Justice

The rapid development of digital technology has significantly transformed criminal justice systems across the world. Technological advancement has changed the manner in which crimes are committed, investigated, prosecuted, and adjudicated. As societies become increasingly dependent on electronic communication and digital infrastructure, criminal procedure systems have also adapted to accommodate new forms of evidence and investigative techniques.

Historically, criminal investigations relied primarily on physical evidence, witness testimony, documentary records, and direct observation. However, the widespread use of computers, mobile devices, internet services, and digital communication has introduced new forms of information that frequently become central to criminal proceedings.

The digital age has created both opportunities and challenges for law enforcement agencies. On one hand, technology enables investigators to collect detailed information regarding communication patterns, financial transactions, location records, surveillance

footage, and electronic activity. Digital forensic methods allow investigators to recover deleted files, reconstruct timelines, and identify connections between individuals and criminal events.

On the other hand, technological advancement has also expanded opportunities for criminal activity. Cybercrime, identity theft, online fraud, unauthorised access to information systems, digital harassment, and technology-assisted offences have become increasingly common. Even traditional offences often involve electronic evidence generated through mobile devices, social media platforms, and digital communication systems.

The emergence of digital evidence has influenced all stages of criminal justice administration. During investigation, authorities now depend on electronic data collection and forensic examination. During prosecution, digital materials are frequently used to support allegations and establish factual relationships. During trial, courts must evaluate the authenticity, reliability, and legal admissibility of electronic records.

Modern criminal justice systems have therefore experienced growing pressure to update procedural rules and evidentiary standards. Traditional legal doctrines often struggle to address questions relating to data preservation, electronic authentication, chain of custody, encryption, and cross-border access to information. These developments require judicial institutions to balance technological efficiency with procedural fairness and protection of fundamental rights.

Digital forensic science has emerged as an important field supporting criminal investigations. Forensic experts use scientific techniques to identify, preserve, analyse, and present electronic information while maintaining evidentiary integrity. Their role has become increasingly important because improper handling of digital evidence may affect reliability and reduce its evidentiary value.

Furthermore, courts have gradually recognised that digital evidence must be evaluated carefully due to its unique characteristics. Questions relating to manipulation, system error, automated generation, and technological dependency continue to influence judicial reasoning.

The relationship between digital technology and criminal justice demonstrates that legal systems must remain adaptable. Effective regulation of digital evidence requires not only technological capability but also strong procedural safeguards to ensure justice, accountability, and public confidence in judicial outcomes.

Accordingly, understanding the development of digital technology within criminal justice provides an important foundation for examining later discussions on admissibility and reliability of digital evidence in criminal trials.

2.4 Review of Existing Literature

The growing use of digital evidence in criminal proceedings has attracted considerable attention from legal scholars, researchers, courts, and policymakers. Existing literature generally recognises that technological advancement has transformed evidentiary practices and created new legal challenges concerning admissibility, authenticity, reliability, and procedural fairness.

Early legal scholarship on evidence law primarily focused on traditional forms of evidence such as oral testimony, documentary records, and physical exhibits. However, the expansion of digital technology led researchers to examine how electronic information should be treated within established evidentiary frameworks. Scholars increasingly argued that conventional legal principles require adaptation to address the unique characteristics of digital data.

A major theme in existing literature concerns the concept of admissibility. Academic discussions frequently emphasise that digital evidence should satisfy traditional evidentiary requirements including relevance, authenticity, and legality of acquisition. At the same time, scholars observe that digital evidence presents additional concerns because electronic information may be altered, duplicated, or manipulated without visible signs of interference.

Another significant area of discussion relates to reliability and authenticity. Researchers highlight that the evidentiary value of digital materials depends heavily on the methods used to collect, preserve, analyse, and present electronic information. Studies repeatedly emphasise the importance of maintaining chain of custody and applying forensic standards to reduce risks of contamination and evidentiary dispute.

Legal literature also addresses challenges associated with digital forensic investigation. Scholars note that modern investigations increasingly depend on technical expertise, specialised software, and forensic examination procedures. As a result, courts may encounter difficulties in evaluating complex technological evidence and balancing expert opinion with legal standards.

Several researchers discuss the relationship between privacy rights and digital investigation practices. Access to electronic records frequently raises concerns regarding personal data protection, surveillance powers, and procedural safeguards. Existing studies argue that effective criminal investigation should not undermine fundamental rights and principles of due process.

Comparative legal studies further indicate that different jurisdictions have adopted varying approaches to electronic evidence regulation. Some legal systems have introduced specific legislative provisions addressing digital evidence, while others continue relying on traditional evidentiary doctrines supported by judicial interpretation.

Academic commentary also highlights concerns regarding technological inequality within justice systems. Investigators, prosecutors, defence lawyers, and courts may not always possess equal access to technical knowledge and forensic resources. This imbalance may affect procedural fairness and influence evidentiary outcomes.

Although existing literature provides extensive discussion regarding electronic evidence and digital investigation, many studies focus either on technical forensic processes or general evidentiary theory. Comparatively fewer studies provide integrated analysis of both admissibility and reliability within the broader context of modern criminal procedure systems.

Accordingly, this research seeks to contribute to existing scholarship by combining legal analysis of admissibility standards with practical examination of reliability challenges and procedural safeguards relating to digital evidence in criminal trials.

2.5 Research Gap and Theoretical Framework

2.5.1 Research Gap

The increasing importance of digital evidence in criminal proceedings has generated substantial academic discussion in recent years. Existing studies have explored various aspects of electronic evidence, digital forensic investigation, cybercrime, and evidentiary standards. However, despite this growing body of literature, several important gaps remain.

Many previous studies concentrate primarily on the technical dimensions of digital forensics, including data recovery, forensic software, and methods of electronic investigation. Although such research contributes significantly to understanding technological processes, it often provides limited analysis of broader legal and procedural concerns affecting criminal trials.

Other legal studies discuss admissibility of electronic evidence by applying traditional rules of evidence. These studies generally focus on legal requirements such as relevance, authenticity, and procedural compliance but give less attention to practical reliability issues arising during collection, preservation, and presentation of digital information.

Similarly, research addressing reliability frequently emphasises technical accuracy without fully examining how courts assess evidentiary trustworthiness within criminal proceedings. Questions concerning chain of custody, judicial interpretation, forensic dependency, privacy concerns, and procedural safeguards remain insufficiently integrated within existing legal analysis.

Another limitation identified in previous scholarship is the fragmented treatment of admissibility and reliability. These concepts are often examined separately even though, in practice, both issues strongly influence one another during criminal trials.

This study seeks to address these limitations by developing an integrated legal analysis of admissibility and reliability of digital evidence within the broader framework of modern criminal procedure systems. The research combines conceptual discussion, procedural evaluation, and practical challenges to provide a more comprehensive understanding of contemporary evidentiary issues.

2.5.2 Theoretical Framework

This research is guided by legal and evidentiary principles that support fair administration of criminal justice.

First, the study applies the Theory of Evidentiary Reliability, which emphasises that evidence should possess sufficient credibility and trustworthiness before influencing judicial decisions. Under this approach, courts must evaluate whether digital evidence accurately reflects factual circumstances and remains free from improper alteration or procedural defects.

Second, the research incorporates the Due Process Theory, which emphasises fairness, legality, and procedural protection within criminal proceedings. According to this perspective, digital evidence should not only support effective law enforcement but also respect procedural safeguards and protect individual rights.

Third, the study draws upon principles of Authenticity and Evidentiary Integrity. These principles require that evidence presented before a court must be genuine and preserved in a manner that prevents manipulation, contamination, or unauthorised modification.

Together, these theoretical approaches provide a framework for analysing the legal acceptance and practical reliability of digital evidence and support the broader objective of strengthening modern criminal procedure systems.

This chapter established the conceptual and academic foundation of the study. The following chapter examines the legal standards governing admissibility of digital evidence in criminal trials.

Chapter Three: Admissibility of Digital Evidence in Criminal Trials

3.1 Concept and Legal Principles of Admissibility

The admissibility of evidence is one of the fundamental principles governing criminal proceedings. It determines whether evidence presented before a court may legally be accepted and considered in deciding the outcome of a case. In modern criminal justice systems, the increasing use of digital evidence has expanded the scope of admissibility analysis and introduced new legal and procedural challenges.

Digital evidence differs from traditional forms of evidence because it exists in electronic form and is created, stored, processed, and transmitted through technological systems. Due to these characteristics, courts often apply both traditional evidentiary principles and additional safeguards when evaluating whether digital materials should be admitted during criminal trials.

In legal practice, admissibility does not automatically guarantee that evidence will be accepted as persuasive. Rather, admissibility determines whether evidence satisfies minimum legal requirements allowing judicial consideration. Once admitted, the court then evaluates the weight and reliability of the evidence.

Several legal principles commonly guide admissibility of digital evidence.

Relevance

The first requirement is relevance. Evidence must demonstrate a logical connection with facts that are material to the issues under determination. Digital evidence should contribute directly or indirectly to proving or disproving allegations presented before the court. Electronic information that lacks probative value may be excluded.

Authenticity

Authenticity is one of the most important requirements for digital evidence. Courts generally require proof that electronic information is genuine and accurately represents its claimed source. Authentication may involve demonstrating ownership of devices, verifying system records, confirming metadata, or presenting forensic examination results.

Integrity

Integrity refers to maintaining evidence in its original condition from collection to courtroom presentation. Since digital data can be altered without visible indication, courts often examine whether appropriate procedures were followed to preserve electronic information and prevent unauthorised modification.

Legality of Collection

Evidence should generally be collected through lawful procedures. Courts may consider whether investigators respected procedural rules, obtained required authorisations, and complied with legal protections relating to privacy and due process. Improperly obtained evidence may affect admissibility.

Chain of Custody

Chain of custody refers to documented procedures showing how evidence was collected, stored, transferred, analysed, and preserved. A complete and reliable chain of custody reduces uncertainty regarding possible alteration or contamination.

Reliability and Judicial Confidence

Although reliability is often considered separately from admissibility, courts frequently examine whether digital evidence appears sufficiently trustworthy to justify admission. Questions concerning technical error, manipulation, automated generation, or forensic weakness may influence judicial decisions.

The admissibility of digital evidence therefore requires balancing technological capability with legal safeguards. Courts must ensure that electronic information contributes to accurate fact-finding while preserving fairness, procedural integrity, and public confidence in criminal justice.

As digital technologies continue to evolve, admissibility standards remain increasingly important in protecting both investigative effectiveness and individual rights within criminal trials.

3.2 Requirements for Admitting Digital Evidence in Criminal Trials

The admissibility of digital evidence in criminal trials depends upon compliance with certain legal and procedural requirements designed to ensure fairness, accuracy, and evidentiary integrity. Because electronic information possesses characteristics that differ from traditional evidence, courts generally apply additional scrutiny before accepting digital materials during judicial proceedings.

The following requirements commonly influence whether digital evidence is admitted in criminal trials.

3.2.1 Relevance of Digital Evidence

Relevance is the primary requirement for admissibility. Digital evidence must relate directly or indirectly to facts in issue and assist the court in determining disputed matters. Electronic information should possess probative value and contribute meaningfully to establishing guilt, innocence, motive, identity, intent, or surrounding circumstances.

Evidence that lacks legal relevance or creates unnecessary confusion may be excluded even if it exists in authentic digital form.

3.2.2 Authenticity and Verification

Authenticity requires proof that digital evidence is genuine and originates from the source claimed by the presenting party. Courts generally seek assurance that electronic information has not been fabricated or falsely attributed.

Authentication may involve:

- Identification of the electronic device;
- Verification of ownership or user control;
- Examination of metadata;
- Digital forensic analysis;
- Expert testimony;
- Confirmation of system records and timestamps.

The inability to establish authenticity may reduce evidentiary value and affect admissibility.

3.2.3 Integrity and Preservation

Integrity requires that digital evidence remain complete and unchanged from the time of collection until presentation before the court. Since electronic information may be modified easily, investigators must preserve original data and maintain secure storage procedures.

Courts often examine whether:

- Original records were protected;
- Copies were accurately created;
- Preservation procedures were followed;
- Access controls were maintained.

Demonstrating evidentiary integrity strengthens judicial confidence.

3.2.4 Proper Collection Procedures

Digital evidence should be obtained through lawful and professionally accepted investigative methods. Investigators are expected to minimise unnecessary alteration and maintain detailed records during evidence collection.

Improper collection procedures may lead to disputes concerning contamination, procedural irregularity, or exclusion of evidence.

3.2.5 Chain of Custody Documentation

Chain of custody is an important procedural requirement for admissibility. It refers to the continuous documentation of possession, transfer, storage, examination, and handling of evidence.

A complete chain of custody generally includes:

- Time and method of collection;
- Identity of persons handling evidence;
- Storage conditions;

• Transfer records;
• Examination procedures.

Weak documentation may create uncertainty regarding evidentiary integrity.

3.2.6 Competence and Expert Examination

Digital evidence frequently requires specialised interpretation. Courts may rely upon digital forensic specialists or expert witnesses to explain technical findings and establish evidentiary credibility.

Expert involvement may assist courts in understanding:

• Data extraction processes;
• System functionality;
• Possibility of manipulation;
• Reliability of forensic methods.

3.2.7 Compliance with Procedural Fairness

Admission of digital evidence should respect broader principles of procedural fairness and due process. Parties should generally receive opportunities to examine, challenge, and respond to electronic evidence presented during trial.

Courts must ensure that technological evidence supports justice rather than undermining fairness.

Overall, admissibility requirements serve as procedural safeguards designed to balance investigative efficiency with legal protection. Proper compliance enhances confidence in digital evidence and supports effective administration of criminal justice.

3.3 Authentication, Chain of Custody, and Evidentiary Integrity

Authentication, chain of custody, and evidentiary integrity are among the most important requirements governing the admissibility of digital evidence in criminal trials. Because digital information may be altered, duplicated, transferred, or manipulated without visible signs, courts frequently rely on these principles to determine whether electronic evidence can be accepted and trusted during judicial proceedings.

3.3.1 Authentication of Digital Evidence

Authentication refers to the process of establishing that digital evidence is genuine and accurately represents the information it claims to contain. Before electronic materials are admitted, the presenting party generally bears responsibility for demonstrating that the evidence originates from an identifiable and reliable source.

Unlike traditional physical evidence, digital evidence often requires additional verification because electronic information may be created anonymously, altered remotely, or reproduced without obvious differences.

Methods commonly used to authenticate digital evidence include:

- Identification of the electronic device or storage source;
- Verification of user ownership or access records;
- Examination of metadata and system information;
- Digital forensic analysis;
- Expert testimony;
- Cross-verification with supporting evidence.

Authentication does not necessarily prove absolute accuracy but establishes a sufficient legal basis for judicial consideration.

3.3.2 Chain of Custody

Chain of custody refers to the documented history of how evidence has been collected, preserved, transferred, examined, stored, and presented from the moment of discovery until courtroom use.

Maintaining chain of custody is particularly important for digital evidence because electronic data may be vulnerable to accidental modification or unauthorised access. A properly documented chain of custody allows courts to trace each stage of evidence handling and evaluate whether integrity has been preserved.

Important elements of chain of custody generally include:

• Identification of the evidence source;
• Date and time of collection;
• Names and responsibilities of handlers;
• Storage procedures;
• Transfer records;
• Documentation of forensic examination;
• Final presentation before court.

Breaks or inconsistencies in chain-of-custody records may reduce confidence in the evidence and create challenges concerning admissibility.

3.3.3 Evidentiary Integrity

Evidentiary integrity refers to maintaining evidence in a complete, accurate, and unchanged condition throughout the legal process. Integrity ensures that the information presented before the court remains substantially identical to the evidence originally collected.

Preserving integrity is particularly challenging for digital evidence because ordinary system operations may unintentionally modify timestamps, metadata, or electronic records.

Measures commonly used to preserve evidentiary integrity include:

• Creating forensic copies rather than altering original data;
• Using secure storage systems;
• Restricting unauthorised access;

• Maintaining documentation of investigative actions;
• Applying standard forensic procedures.

Judicial confidence in digital evidence often depends on the ability to demonstrate evidentiary integrity.

3.3.4 Relationship Between Authentication, Chain of Custody, and Integrity

Although these concepts are distinct, they operate together during criminal proceedings. Authentication establishes that evidence is genuine, chain of custody documents handling procedures, and integrity ensures that the evidence remains unchanged.

Failure in any one of these areas may weaken evidentiary value and influence judicial decisions regarding admissibility and reliability.

Accordingly, effective management of authentication, chain of custody, and evidentiary integrity has become essential in modern criminal procedure systems where digital evidence increasingly shapes criminal adjudication.

3.4 Judicial Challenges in Admitting Digital Evidence

The increasing use of digital evidence in criminal proceedings has created significant challenges for courts and judicial institutions. Although electronic information offers valuable investigative opportunities, judges frequently encounter difficulties when determining whether such evidence satisfies legal standards of admissibility. These challenges arise because digital evidence differs substantially from traditional forms of evidence and often requires both legal and technical evaluation.

3.4.1 Difficulty in Verifying Authenticity

One of the most significant judicial challenges concerns authentication of digital evidence. Courts must determine whether electronic records genuinely originate from the claimed source and whether they accurately represent relevant events.

Unlike physical documents, digital information may be copied, edited, fabricated, or generated using automated systems without obvious signs of alteration. As a result, judges often depend upon technical reports, metadata analysis, and expert testimony to establish authenticity.

3.4.2 Risk of Manipulation and Alteration

Digital evidence may be vulnerable to intentional or accidental modification during collection, storage, transfer, or analysis. Electronic files can sometimes be changed without leaving visible indications.

This possibility creates difficulties for courts because judges must determine whether evidence presented during trial remains identical to the original information collected by investigators.

3.4.3 Technical Complexity

Modern criminal proceedings increasingly involve technologically complex evidence. Judges and legal practitioners may not always possess specialised technical knowledge necessary to interpret electronic records, forensic reports, or digital investigation methods.

Dependence on technical experts may create challenges regarding evaluation of expert credibility and understanding of forensic methodology.

3.4.4 Weaknesses in Chain of Custody

Courts frequently examine whether digital evidence has been properly documented throughout investigative procedures. Missing records, unclear transfer processes, incomplete documentation, or improper storage may reduce judicial confidence.

Even minor procedural irregularities may generate disputes regarding admissibility and reliability.

3.4.5 Balancing Privacy and Investigation

Digital investigations often involve access to personal devices, communication records, online accounts, and electronic databases. Courts must therefore balance effective criminal investigation with protection of privacy and procedural rights.

Excessive or unlawful access to electronic information may create legal concerns and influence evidentiary decisions.

3.4.6 Cross-Border and Jurisdictional Difficulties

Digital evidence frequently exists beyond geographical boundaries. Cloud storage systems, international communication networks, and foreign service providers may complicate evidence collection and judicial authority.

Courts may encounter difficulties concerning legal cooperation, jurisdiction, and recognition of foreign electronic records.

3.4.7 Dependence on Expert Testimony

Judicial assessment of digital evidence often relies heavily on forensic specialists and technical experts. However, competing expert opinions, differences in methodology, and limitations of forensic tools may complicate evidentiary evaluation.

Judges must ensure that expert evidence supports rather than replaces independent judicial reasoning.

3.4.8 Rapid Technological Change

Technology evolves faster than legal reform in many jurisdictions. Courts sometimes apply traditional evidentiary principles to modern technological environments, creating uncertainty and inconsistency.

Judicial institutions therefore face continuing pressure to adapt procedural standards and maintain effective regulation of electronic evidence.

Overall, judicial challenges in admitting digital evidence demonstrate the need for stronger procedural safeguards, improved forensic standards, judicial training, and continuous legal development. Addressing these challenges is essential for maintaining fairness, reliability, and public confidence in modern criminal justice systems.

3.5 Comparative and Critical Analysis of Admissibility Standards

The growing dependence on digital evidence has encouraged legal systems across the world to reconsider traditional evidentiary approaches and develop standards capable of responding to technological change. Although jurisdictions differ in procedural structure and legal tradition, many share common concerns regarding authenticity, reliability, legality of collection, and protection of procedural rights.

Traditional evidence law was originally developed to regulate physical documents, witness testimony, and tangible exhibits. Digital evidence challenged these conventional frameworks because electronic information may exist in multiple locations simultaneously, be altered without visible signs, and require specialised examination.

Many modern criminal procedure systems have responded by recognising that traditional principles remain relevant but require adaptation for technological contexts. Courts increasingly apply broader standards that combine relevance, authenticity, integrity, and procedural compliance when evaluating digital evidence.

A comparative review of legal approaches demonstrates several common trends.

First, there is increasing recognition of authenticity requirements. Courts generally expect parties presenting digital evidence to establish its origin and demonstrate that electronic records have not been materially altered. Authentication mechanisms often involve metadata examination, forensic analysis, documentary records, and expert testimony.

Second, legal systems increasingly emphasise evidentiary integrity. Preservation procedures and chain-of-custody documentation have become central requirements because courts seek assurance that electronic information remains substantially unchanged throughout investigation and prosecution.

Third, procedural fairness remains a consistent concern. Criminal justice systems generally recognise that parties should have meaningful opportunities to examine and challenge digital evidence. Judicial transparency and equality between prosecution and defence continue to influence admissibility decisions.

Despite these developments, several weaknesses remain visible across contemporary legal approaches.

One criticism concerns excessive dependence on technical expertise. Courts frequently rely on forensic specialists to interpret electronic evidence, which may create difficulties where judges and legal practitioners possess limited technological understanding.

Another concern relates to inconsistency in judicial practice. Because digital evidence continues to evolve rapidly, similar categories of electronic information may receive different treatment across cases depending upon available expertise, procedural standards, and judicial interpretation.

Additionally, legal reform often develops more slowly than technological innovation. Existing procedural rules may not always provide detailed guidance regarding cloud-based evidence, automated systems, artificial intelligence, encrypted communication, or cross-border electronic investigations.

A critical analysis suggests that effective admissibility standards should not focus exclusively on technological capability. Instead, courts should maintain a balanced approach that integrates legal certainty, evidentiary reliability, procedural fairness, and protection of individual rights.

Improving admissibility standards may require:

- Clear legislative guidance regarding digital evidence;
- Strong authentication procedures;
- Standardised forensic practices;
- Improved judicial and investigative training;
- Enhanced chain-of-custody protocols;
- Greater institutional capacity for handling electronic information.

This chapter examined the legal principles governing admissibility of digital evidence and analysed the challenges courts face when evaluating electronic materials during criminal trials. The following chapter explores issues relating to reliability and practical challenges within modern criminal procedure systems.

CHAPTER FOUR
RELIABILITY CHALLENGES IN MODERN CRIMINAL PROCEDURE SYSTEMS

4.1 Concept of Reliability and Its Importance in Digital Evidence

Reliability is one of the most important considerations in determining the evidentiary value of digital evidence in criminal trials. While admissibility determines whether evidence may legally be accepted by a court, reliability concerns whether the evidence can be trusted as an accurate representation of facts. In modern criminal procedure systems, reliability has become increasingly important because digital evidence frequently influences judicial findings and criminal outcomes.

Digital evidence possesses unique characteristics that distinguish it from traditional forms of evidence. Electronic information may be generated automatically, transmitted instantly, duplicated without visible changes, altered remotely, or stored across multiple technological environments. These characteristics create both opportunities and risks within criminal proceedings.

Reliability generally refers to the degree of confidence that evidence accurately reflects the original information and remains free from distortion, manipulation, technical error, or procedural irregularity. Reliable evidence supports accurate judicial decision-making and strengthens public confidence in the administration of justice.

In criminal trials, reliable digital evidence may assist courts in:

- Establishing timelines of criminal events;
- Confirming communication between individuals;
- Identifying suspects and locations;
- Supporting or challenging witness testimony;
- Demonstrating intent, conduct, or patterns of behaviour.

However, reliability concerns arise because digital evidence often depends upon technological processes rather than direct human observation. Errors may occur during data extraction, software processing, forensic examination, storage, transfer, or courtroom presentation.

One important factor affecting reliability is data integrity. If digital information is modified intentionally or unintentionally after collection, courts may question whether the evidence accurately reflects original conditions. Similarly, incomplete documentation or weak preservation procedures may reduce confidence in evidentiary value.

Reliability is also influenced by technical competence. Investigators, forensic specialists, prosecutors, defence lawyers, and judges may interpret electronic evidence differently depending on expertise and available resources. Differences in technological understanding may create uncertainty during judicial evaluation.

Another challenge involves automated and algorithmic systems. Certain digital records are generated through software processes rather than direct human activity. Courts may therefore need to evaluate system accuracy, operational reliability, and limitations of technological tools.

Modern criminal procedure systems increasingly recognise that reliability cannot be assumed simply because information exists electronically. Instead, reliability must be demonstrated through proper procedures, forensic safeguards, documentation, and judicial scrutiny.

Accordingly, reliability serves as a foundational principle that supports evidentiary credibility, procedural fairness, and effective administration of criminal justice. Understanding reliability is essential for evaluating the broader challenges associated with digital evidence in contemporary criminal trials.

4.2 Risks of Manipulation, Alteration, and Technical Error

One of the most significant challenges affecting the reliability of digital evidence in criminal trials is the possibility of manipulation, alteration, and technical error. Unlike traditional physical evidence, digital information may be modified, duplicated, deleted, or corrupted in ways that are not immediately visible. These characteristics create important concerns regarding evidentiary trustworthiness and judicial confidence.

Digital evidence often passes through multiple stages before being presented in court, including identification, collection, extraction, preservation, storage, examination, and presentation. At each stage, there is a possibility that evidence may be affected intentionally or unintentionally.

4.2.1 Manipulation of Digital Evidence

Manipulation refers to deliberate actions taken to modify electronic information in order to conceal, distort, fabricate, or influence evidentiary value. Advances in technology have increased opportunities for altering digital records through editing software, remote access systems, automated processes, and unauthorised intervention.

Examples of manipulation may include:

- Editing electronic documents;
- Modifying digital photographs or video recordings;
- Altering timestamps and metadata;
- Deleting communication records;
- Creating fabricated digital content.

Such actions may significantly affect judicial assessment and create risks of wrongful legal outcomes.

4.2.2 Accidental Alteration and Data Corruption

Not all changes to digital evidence occur intentionally. Electronic information may be altered accidentally during normal system operations or investigative procedures.

Examples include:

- Opening files without protective procedures;
- Improper data transfer methods;
- Device malfunction;

• Software incompatibility;
• Storage failure.

Even small unintended modifications may affect metadata and raise concerns regarding authenticity and reliability.

4.2.3 Technical Errors in Collection and Analysis

Technical limitations may also reduce reliability of digital evidence. Errors can occur during forensic acquisition, software processing, data extraction, interpretation, or report preparation.

Common technical issues include:

• Incomplete recovery of electronic records;
• Incorrect forensic settings;
• Misinterpretation of extracted data;
• Software malfunction;
• Inaccurate system output.

These challenges demonstrate that technology itself cannot guarantee evidentiary accuracy.

4.2.4 Metadata Distortion

Metadata provides important contextual information such as creation dates, modification history, access records, and device information. However, metadata may change automatically during ordinary system activity.

If metadata becomes inaccurate or incomplete, courts may experience difficulty establishing timelines and confirming authenticity.

4.2.5 Impact on Criminal Proceedings

Manipulation, alteration, and technical error may create serious consequences within criminal justice systems. Courts may question evidentiary credibility, exclude evidence from consideration, or assign reduced evidentiary weight.

These risks may also affect procedural fairness by limiting opportunities for effective challenge and increasing dependence on technical expertise.

4.2.6 Preventive Measures

To reduce reliability concerns, criminal justice systems increasingly emphasise:

- Standardised evidence collection procedures;
- Digital forensic protocols;
- Secure storage mechanisms;
- Controlled access to electronic records;
- Comprehensive documentation practices;
- Independent verification and review.

These measures strengthen confidence in digital evidence and support fair judicial outcomes.

Overall, risks of manipulation, alteration, and technical error represent major obstacles to evidentiary reliability. Addressing these concerns remains essential for maintaining trust in digital evidence within modern criminal procedure systems.

4.3 Chain of Custody, Forensic Examination, and Reliability Assurance

The reliability of digital evidence in criminal trials depends heavily upon proper preservation procedures, scientific examination, and transparent evidentiary management. Among the most important mechanisms supporting evidentiary reliability are chain of custody and forensic examination. These processes help ensure that digital evidence remains authentic, accurate, and suitable for judicial consideration.

Because electronic information can be modified easily and often lacks visible indicators of alteration, criminal justice systems increasingly require structured procedures to preserve evidentiary integrity from the initial stage of investigation through final courtroom presentation.

4.3.1 Role of Chain of Custody in Reliability

Chain of custody refers to the continuous and documented process that records how evidence is identified, collected, transferred, stored, analysed, and presented throughout criminal proceedings.

The primary objective of chain of custody is to establish confidence that digital evidence has remained substantially unchanged and has not been exposed to unauthorised access or procedural irregularity.

An effective chain-of-custody process generally includes:

- Identification of the evidence source;
- Documentation of collection procedures;
- Recording dates and times of handling;
- Maintaining transfer records;
- Secure storage procedures;
- Preservation of examination history.

Strong chain-of-custody documentation allows courts to trace evidentiary movement and evaluate reliability.

4.3.2 Importance of Digital Forensic Examination

Digital forensic examination refers to the systematic process of identifying, preserving, analysing, and interpreting electronic information for legal purposes.

Forensic examination supports reliability by applying structured scientific methods designed to minimise alteration and maximise evidentiary accuracy.

Key stages of forensic examination commonly include:

- Identification of digital sources;
- Preservation of original information;

• Creation of forensic copies;
• Technical analysis of electronic records;
• Documentation of findings;
• Preparation of expert reports.

Forensic methods assist courts in understanding technical evidence while maintaining procedural integrity.

4.3.3 Reliability Assurance Through Standard Procedures

Reliability assurance involves implementing safeguards that reduce risks of contamination, loss, and evidentiary dispute.

Important reliability measures include:

• Use of validated forensic tools;
• Controlled access to digital records;
• Independent review of technical findings;
• Preservation of original data;
• Consistent investigative protocols.

These measures strengthen confidence that electronic information accurately reflects original circumstances.

4.3.4 Challenges Affecting Reliability Assurance

Despite procedural safeguards, several challenges continue to affect reliability.

These include:

• Human error during evidence handling;
• Incomplete documentation;
• Technological limitations;

• Rapid changes in software environments;
• Dependence on specialised expertise.

Inadequate training or inconsistent procedures may reduce evidentiary value and increase judicial uncertainty.

4.3.5 Judicial Evaluation of Reliability

Courts generally evaluate reliability by considering:

• Whether collection procedures were documented;
• Whether evidence remained protected from interference;
• Whether forensic methods appear credible;
• Whether opposing parties had opportunities to challenge findings.

Judicial assessment therefore extends beyond technical examination and includes broader considerations of procedural fairness and evidentiary trustworthiness.

Overall, chain of custody and forensic examination remain essential mechanisms for maintaining reliability of digital evidence. Their effective application contributes to accurate judicial outcomes and strengthens public confidence in modern criminal justice systems.

4.4 Privacy, Procedural Fairness, and Human Rights Concerns

The increasing use of digital evidence in criminal trials has created important legal and ethical questions concerning privacy, procedural fairness, and protection of human rights. Although digital technologies provide valuable investigative opportunities, their use must remain consistent with fundamental principles of justice and legal accountability.

Digital evidence frequently originates from personal devices, communication systems, internet activity, cloud services, and electronic databases. These sources often contain extensive private information beyond the scope of a particular investigation. As a result, criminal procedure systems must balance effective law enforcement with respect for individual rights.

4.4.1 Privacy Concerns in Digital Investigation

Privacy is a fundamental legal value that protects individuals from unnecessary interference with personal information and private life. Digital investigations often require access to sensitive electronic records including messages, photographs, location history, browsing activity, and personal communications.

Because electronic devices may contain extensive personal data, investigators face challenges in limiting evidence collection to information directly relevant to criminal proceedings.

Privacy concerns commonly arise in situations involving:

- Access to mobile devices;
- Collection of communication records;
- Surveillance technologies;
- Remote searches and cloud-based information;
- Long-term electronic monitoring.

Failure to respect privacy protections may affect public trust and create legal challenges concerning admissibility.

4.4.2 Procedural Fairness in Criminal Proceedings

Procedural fairness is a central principle of criminal justice. It requires that legal procedures remain transparent, impartial, and consistent with due process.

When digital evidence is introduced during criminal trials, fairness concerns may arise if parties do not receive adequate opportunities to examine, challenge, or understand electronic materials.

Procedural fairness generally requires:

- Timely disclosure of evidence;
- Access to relevant electronic records;

• Opportunity to question expert findings;
• Equality between prosecution and defence;
• Transparent evidentiary procedures.

Courts must ensure that technological complexity does not create procedural imbalance.

4.4.3 Human Rights Considerations

The use of digital evidence may also affect broader human rights principles. Criminal investigations must maintain respect for legal protections including dignity, liberty, fair trial rights, and protection from arbitrary interference.

Human rights concerns become particularly important where digital surveillance or extensive data collection occurs without adequate safeguards.

Important considerations include:

• Respect for personal autonomy;
• Limitation of investigative powers;
• Judicial oversight mechanisms;
• Protection against unlawful intrusion;
• Accountability in evidence collection.

Balancing investigative necessity with rights protection remains an ongoing challenge.

4.4.4 Risks of Excessive Technological Dependence

Modern criminal justice systems increasingly depend on technological systems and digital investigation tools. However, excessive dependence may reduce transparency and create difficulties for judicial review.

Courts must remain cautious when relying heavily on automated systems, complex forensic methods, or technical conclusions that parties cannot effectively challenge.

4.4.5 Strengthening Rights-Based Approaches

To address these concerns, criminal procedure systems increasingly encourage:

• Clear legal standards for digital investigation;
• Independent judicial supervision;
• Data protection safeguards;
• Enhanced procedural transparency;
• Opportunities for evidentiary challenge.

Such measures support both effective criminal investigation and protection of individual rights.

Overall, privacy, procedural fairness, and human rights considerations remain essential elements in evaluating reliability of digital evidence. Effective criminal justice requires not only technological efficiency but also continuous protection of legal and constitutional values.

Chapter Five: Findings, Recommendations and Conclusion

This chapter summarises findings and recommends stronger legal frameworks and procedural safeguards.

5.1 Major Findings of the Study

This research examined the admissibility and reliability of digital evidence in criminal trials and analysed the challenges faced by modern criminal procedure systems in managing electronic information. Based on the discussion presented in previous chapters, several major findings emerged.

First, the study found that digital evidence has become an increasingly important component of criminal justice administration. Modern criminal investigations and trials rely extensively on electronic information generated through communication technologies, digital devices, surveillance systems, and internet-based activities. Digital evidence now frequently supports identification of suspects, reconstruction of events, and judicial decision-making.

Second, the study found that traditional evidentiary principles continue to play an important role in evaluating digital evidence. Requirements relating to relevance, authenticity, integrity, legality of collection, and procedural fairness remain essential for determining admissibility. However, these principles require adaptation to address the unique nature of electronic information.

Third, the research demonstrated that reliability represents one of the most significant concerns associated with digital evidence. Unlike conventional forms of evidence, digital information may be altered, duplicated, manipulated, or corrupted without obvious physical indication. As a result, courts must apply greater scrutiny before relying upon electronic materials.

Fourth, the study identified authentication and chain of custody as critical mechanisms supporting evidentiary trustworthiness. Proper documentation, secure preservation procedures, and transparent handling practices strengthen judicial confidence and reduce challenges concerning evidentiary integrity.

Fifth, the research revealed that technical expertise plays an increasingly important role in criminal proceedings involving digital evidence. Investigators, forensic specialists, prosecutors, and judges often depend upon specialised knowledge to interpret electronic information and assess reliability.

Sixth, the study found that privacy and procedural fairness remain fundamental concerns. Effective criminal investigation should not compromise legal protections or limit opportunities for parties to challenge digital evidence presented during trial.

Finally, the research concluded that many criminal procedure systems continue to experience difficulties adapting legal standards to rapidly developing technological environments. Ongoing reform and institutional development remain necessary.

These findings establish the basis for the recommendations presented in the following section.

5.2 Recommendations

Based on the findings and analysis presented throughout this study, several recommendations are proposed to strengthen the admissibility and reliability of digital evidence in criminal trials and improve the effectiveness of modern criminal procedure systems.

1. Development of Clear Legal Frameworks

Legislative authorities should establish clear and updated legal provisions governing the collection, preservation, authentication, and admissibility of digital evidence. Modern procedural rules should address emerging technological realities while maintaining consistency with fundamental principles of justice.

2. Strengthening Authentication Procedures

Courts and investigative agencies should adopt stronger authentication standards to verify the origin and integrity of electronic information. Standardised verification methods may reduce disputes regarding authenticity and increase confidence in judicial outcomes.

3. Improvement of Chain-of-Custody Practices

Criminal justice institutions should strengthen documentation procedures for handling digital evidence. Comprehensive records concerning collection, transfer, storage, examination, and presentation should be maintained throughout criminal proceedings.

4. Expansion of Digital Forensic Capacity

Governments and relevant institutions should invest in developing forensic infrastructure and improving technical capability. Reliable forensic examination supports evidentiary accuracy and reduces risks associated with improper handling.

5. Professional Training and Capacity Building

Judges, prosecutors, investigators, and legal practitioners should receive continuous education regarding digital evidence and technological developments. Improved understanding may strengthen judicial evaluation and procedural consistency.

6. Standardisation of Investigative Procedures

Investigative authorities should adopt uniform procedures and operational guidelines for managing electronic information. Standardisation may reduce evidentiary disputes and improve institutional efficiency.

7. Protection of Privacy and Procedural Rights

Digital investigation methods should remain consistent with principles of privacy, procedural fairness, and protection of individual rights. Legal safeguards should ensure that investigative powers remain proportionate and accountable.

8. Increased Judicial Oversight

Courts should exercise active supervision regarding collection and use of digital evidence. Judicial review strengthens accountability and protects against improper evidentiary practices.

9. Encouragement of Interdisciplinary Cooperation

Effective management of digital evidence requires cooperation among legal professionals, forensic specialists, technical experts, policymakers, and academic institutions. Collaborative approaches may improve institutional responses to technological change.

10. Continuous Legal Reform

Because technology develops rapidly, legal systems should periodically review evidentiary rules and procedural standards to maintain relevance and effectiveness.

Implementation of these recommendations may contribute to stronger evidentiary standards, greater procedural fairness, and improved public confidence in criminal justice administration.

5.3 Conclusion

This study examined the admissibility and reliability of digital evidence in criminal trials and analysed the challenges that arise within modern criminal procedure systems. The research demonstrated that rapid technological development has significantly transformed criminal investigation and judicial practice, making digital evidence an increasingly important element of contemporary criminal justice.

The study established that digital evidence now plays a central role in criminal proceedings because modern communication systems, electronic devices, surveillance technologies, and digital platforms generate large amounts of potentially valuable information. Electronic records may assist courts in reconstructing events, identifying offenders, verifying testimony, and supporting legal decision-making.

However, the research also demonstrated that the growing use of digital evidence creates substantial legal and procedural concerns. Unlike traditional forms of evidence, digital information possesses characteristics that increase vulnerability to alteration, duplication, manipulation, and technical error. These risks require stronger safeguards to maintain evidentiary reliability and protect procedural fairness.

The analysis showed that admissibility remains dependent upon core evidentiary principles including relevance, authenticity, integrity, legality of collection, and procedural compliance. Courts must ensure that digital evidence satisfies legal requirements before accepting it during criminal proceedings.

The study further emphasised that reliability extends beyond technical accuracy. Reliable digital evidence requires proper preservation procedures, transparent chain of custody, professional forensic examination, effective judicial oversight, and opportunities for parties to challenge evidentiary claims.

Another important conclusion of the study is that technological progress continues to outpace legal development in many criminal justice systems. Existing evidentiary frameworks often require adaptation to respond effectively to changing technological conditions while preserving constitutional values and fair trial standards.

This research therefore supports the position that successful integration of digital evidence into criminal trials requires a balanced approach that combines technological advancement with legal accountability. Criminal procedure systems should continue strengthening procedural safeguards, developing institutional capacity, and updating evidentiary standards to ensure fair and reliable judicial outcomes.

In conclusion, digital evidence will continue to shape the future of criminal justice. The effectiveness of modern criminal procedure systems will increasingly depend upon their ability to maintain admissibility standards, protect reliability, and uphold principles of justice in an evolving technological environment.

BIBLIOGRAPHY

A. BOOKS

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Mason, S. (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies.

Roberts, P., & Zuckerman, A. (2010). *Criminal evidence* (2nd ed.). Oxford University Press.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2011). *Digital evidence in criminal investigations*. International Journal of Digital Crime and Forensics.

Murphy, E. (2007). *The new forensics: Criminal justice, false certainty, and scientific evidence*. California Law Review.

Ziccardi, G. (2019). *Digital evidence and electronic signature law*. Springer.

B. JOURNAL ARTICLES

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. *Columbia Law Review, 105*(1), 279–318.

Pollitt, M. (2010). An ad hoc review of digital forensic models. *Digital Investigation, 7*(1–2), 1–12.

Williams, M. (2015). Evidence and criminal procedure in the digital age. *Legal Studies Review, 34*(2), 95–114.

Goodison, S., Davis, R., & Jackson, B. (2015). Digital evidence and the U.S. criminal justice system. *RAND Justice Reports*.

C. INTERNATIONAL REPORTS AND DOCUMENTS

United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive study on cybercrime*.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.

National Institute of Standards and Technology (NIST). (2014). *Guidelines on mobile device forensics*.

D. LEGISLATION

Evidence Act.

Code of Criminal Procedure.

Information and Communication Technology Act.

Digital Security Act.

Relevant national electronic evidence regulations and procedural laws.

E. CASE STUDIES / CASE LAW

1. *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (2007).
   This case discussed admissibility standards for electronically stored information and emphasised authentication requirements.
2. *R v. Shepherd* [1993] AC 380.
   The court considered reliability and admissibility of computer-generated evidence.
3. *Riley v. California*, 573 U.S. 373 (2014).
   The case examined digital privacy and electronic search principles involving mobile devices.
4. *State v. Pratt* (Digital Forensic Evidence Case).
   The case highlighted chain-of-custody and forensic examination concerns.
5. *United States v. Ganias*, 755 F.3d 125 (2014).
   The decision examined retention and use of copied digital records during criminal investigation.
6. *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
   This case established important principles regarding admissibility of electronic evidence.

7. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020).
   The judgment clarified procedural requirements concerning electronic evidence certification.

F. ONLINE AND ELECTRONIC SOURCES

Academic databases, law journals, university repositories, government publications, and official legal materials consulted during preparation of this research.

References (APA)

Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105(1), 279–318.

Mason, S. (2017). Electronic evidence (4th ed.). Institute of Advanced Legal Studies.

Murphy, E. (2007). The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence. California Law Review, 95(3), 721–797.

Pollitt, M. (2010). An ad hoc review of digital forensic models. Digital Investigation, 7(1–2), 1–12.

Schjølberg, S., & Ghernaouti, H. (2011). A global treaty on cybersecurity and cybercrime. Cybercrime Research Institute.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2011). Digital evidence in criminal investigations. International Journal of Digital Crime and Forensics.

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime.

Williams, M. (2015). Evidence and criminal procedure in the digital age. Legal Studies Review. Ziccardi, G. (2019). Digital evidence and electronic signature law. Springer.