International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 4, Number: 2, Pages: 118 - 125, Year: 2025

Cybersecurity Challenges in Digital Forensics Types: Network Forensics, Cloud Forensics and Mobile Forensics

Sidra Khan*, Irshad Ahmed Sumra, Bilal Gillani, and Waqar Azeem

Department of Informatics and Systems, School of Systems and Technology, University of Management and Technology Lahore, 54000, Pakistan
*Corresponding author: Sidra Khan (Email: sidrashuebkhan@gmail.com)

Received: 12/10/2025, Revised: 22/11/2025, Accepted: 25/12/2025

***Abstract*— The rapid growth of information and communication technologies (ICTs) has increased the risk of cybercrime, data breaches, ransomware attacks, and other cybersecurity threats. Digital forensics plays a crucial role in investigating cyber incidents by collecting, preserving, analyzing, and presenting digital evidence from various digital environments. This review paper discusses the concept of digital forensics and its major types, including network, cloud, and mobile forensics. It highlights the importance of these forensic domains in identifying cyber threats, supporting investigations, and enhancing cybersecurity. The paper also examines key challenges related to digital investigations, ransomware attacks, Internet of Things (IoT) environments, and emerging technologies. Furthermore, it reviews recent research developments and future directions aimed at improving forensic capabilities, evidence management, and cybersecurity defenses in modern digital systems.**

***Index Terms*—Digital Forensics, Network Forensics, Cloud Forensics, Mobile Forensics, Cybersecurity, Digital Evidence, Cybercrime, Ransomware, IoT Security.**

I. INTRODUCTION

Digital technologies have revolutionized society today. Modern computer networks, cloud computing platforms, mobile devices, and Internet-based services are critical to the communications, data storage, financial transactions, and business operations of organizations. The progress the technologies are making in improving lives, on the other hand, creates opportunities for cybercriminals to exploit vulnerabilities and initiate sophisticated cyberattacks. These types of cyberattacks have become more frequent and are causing significant economic and reputational impacts on organisations worldwide [1]. Traditional security systems are not enough to block and track attacks due to the growing scale and sophistication of cybercrime. Digital forensics has become an indispensable aspect of cybersecurity, enabling the collection, analysis, and preservation of digital evidence related to cyber incidents. Digital forensic investigations assist not only in identifying attackers but also in reconstructing attack scenarios, understanding their impact, and presenting reliable evidence to support legal proceedings [2].

Digital Forensics is an interdisciplinary field that includes computer science, information security, law enforcement, and legal protocols. It covers many specialized areas such as computer forensics, network forensics, cloud forensics, and mobile forensics. There are different challenges for collecting and analyzing evidence from different technological environments [3], and each domain handles a unique set of them. The use of cloud computing, Internet of Things (IoT) devices, Artificial Intelligence (AI), and mobile technologies has created a wide range of new areas of digital investigation. As a result, researchers and practitioners are actively developing new forensic techniques and tools to address emerging challenges and enhance cybersecurity resilience [4].

This review differs from current review studies on specific aspects of digital forensics, such as network forensics, cloud forensics, or ransomware analysis, in that it provides a broad perspective on the field as a whole. The paper draws together cutting-edge concepts such as ransomware investigations, Internet of Things (IoT) forensics, preservation of evidence in blockchain networks, and AI-driven forensics into the world of network, cloud, and mobile. Furthermore, studies in related areas were discussed, and a comparative study was conducted to identify current trends, limitations, and future research needs. Unlike past survey articles, this broader view provides a clearer picture of the field and thus serves as a better reference for researchers and practitioners in digital forensics and cybersecurity.

The rest of this paper is organized as follows. Section II presents the concept and importance of digital forensics, while Section III discusses the digital forensic investigation process. Section IV introduces the major types of digital forensics, including network, cloud, and mobile forensics. Sections V, VI, and VII provide detailed discussions of network, cloud, and mobile forensics, respectively. Section VIII highlights the

major cybersecurity challenges associated with digital forensic investigations. Sections IX examine ransomware analysis and IoT forensic challenges. Section X presents a comparative analysis of existing studies, followed by future research directions in Section XI. Finally, Section XII concludes the paper and summarizes the key findings.

II. Concept of Digital Forensics

Digital forensics is the systematic discipline of identifying, acquiring, preserving, examining, analysing, and presenting digital evidence from digital devices and systems. The primary objective of digital forensics is to conduct investigations of cyber incidents and deliver reliable digital evidence that is suitable for legal and organizational decision-making processes [3]. Digital evidence can come from multiple sources, including computer systems, servers, smartphones, cloud systems, network devices, databases, and Internet-connected devices. Digital evidence can be easily altered, deleted, or destroyed, and is more volatile than traditional physical evidence. Consequently, the procedures and methods monitored by forensic investigators should be strictly followed to ensure the integrity and authenticity of the evidence collected [5]. With the increasing prevalence of cybercrime, the role of digital forensics has become a critical role. Digital Forensics techniques are employed to investigate information breaches, insider threats, IP theft, fraud, ransomware events, and unauthorized access. Digital forensics is also used by law enforcement agencies to support the investigation of cybercrimes, comprising cybercriminal activities [6].

A successful digital forensic investigation typically seeks to answer several critical questions:

- Who performed the malicious activity?
- What actions were carried out?
- When did the incident occur?
- Where did the attack originate?
- Why was the attack conducted?
- How were vulnerabilities exploited?

Investigators can use these questions to reconstruct cyber incidents, determine who is accountable, and suggest ways to prevent future incidents [3].

III. Digital Forensic Investigation Process

Digital forensic investigations are conducted using a systematic methodology to ensure the integrity, authenticity, and admissibility of digital evidence. One of the most widely recognized investigation models (Fig. 1) is the Integrated Digital Investigation Process (IDIP), proposed by Carrier and Spafford [7].

A. Readiness Phase

The readiness phase focuses on preparing investigation teams, infrastructure, organizational policies, and forensic tools before security incidents occur. During this phase, forensic procedures are established, investigators are provided with appropriate training, and monitoring systems are deployed to collect and preserve relevant digital evidence [7].

Fig. 1: Workflow of the Digital Forensic Investigation Process

B. Deployment Phase

The deployment phase begins when a security incident is identified. Investigators assess the nature and scope of the incident to determine whether a forensic investigation is required. Initial evidence collection and incident documentation activities are also initiated during this phase.

C. Physical Investigation Phase

This phase involves the examination of physical devices, storage media, and hardware associated with the incident. Digital evidence is secured, and the physical crime scene is carefully documented to maintain the integrity of the investigation.

D. Digital Investigation Phase

In this phase, investigators analyze digital evidence from all types of computer systems, networks, mobile devices, and cloud environments. Specialized Forensic tools are utilized to recover deleted data, to detect attack patterns, and reconstruct the chronological sequence of events related to the incident.

E. Review Phase

The final phase involves evaluating the investigation's effectiveness and identifying opportunities to improve forensic procedures and strengthen cybersecurity practices for future incident response.

F. Types of Digital Forensics

Digital forensics is a collection of specialized disciplines that operate across various technological environments. Among these, network, clous, and mobile forensics are considered the most relevant domains in modern cybersecurity (Fig. 2).

IV. Network Forensics

Network forensics involves the collection, documentation, monitoring, and analysis of network data to investigate security incidents and detect malicious activities. It focuses on collecting evidence from communication networks rather than individual devices [3].

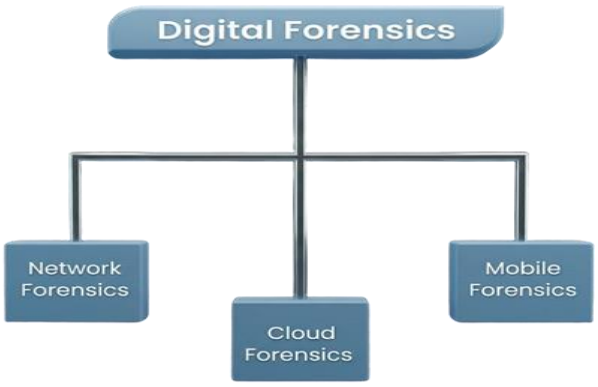

Figure 2. Classification of Digital Forensics Domains

Mazurczyk et al. [1] stated that modern societies heavily depend on communication networks for business, government services, and personal communication. This dependency has exposed these networks to cyber threats, making network forensics an important component of cybersecurity. Network forensic investigations include the analysis of network packets, communication logs, traffic flows, and intrusion detection system (IDS) alerts. These sources of evidence enable investigators to determine the origin of an attack, reconstruct its timeline, and understand how the attack was carried out.

Applications of Network Forensics: The applications of network forensics include detecting cyberattacks, investigating data breaches, analysing malware and ransomware, conducting insider threat investigations, and collecting evidence for legal proceedings.

Several advanced methods have been proposed to enhance network forensic capabilities. Filasiak et al. [6] developed realistic datasets to evaluate cyber threat detection systems, while Cheng et al. [7] developed the CHEETAH framework to reduce the storage requirements of network forensic analysis.

Ransomware investigations also rely heavily on network forensics. To improve ransomware detection, Sharmila and Chaudhari [18] proposed combining network forensic analysis with threat intelligence platforms. Similarly, Choo et al. [19] reported that analysing malicious URLs and network indicators can be used to detect cyber threats. Despite its importance, network forensics faces several limitations, including the massive volume of network data, encrypted communications, privacy concerns, and increasingly complex network environments [11].

V. Cloud Forensics

Cloud forensics is a specialized area of digital forensics that focuses on investigating incidents in cloud computing environments. Organizations worldwide have adopted cloud computing because it provides scalable storage, processing power, and remote access capabilities. However, these advantages also introduce new forensic challenges [11].

Cloud forensic investigations differ significantly from traditional forensic investigations because data is distributed across multiple servers, geographical locations, and virtualized environments. As a result, accessing logs, maintaining the chain of custody, and determining data ownership can become challenging [12].

The most common steps to cloud forensics are evidence identification, evidence acquisition, data preservation, log analysis, and incident reconstruction. Forensic applications have been proposed to enhance evidence preservation and integrity in blockchain-based cloud and IoT environments. Hossain et al. [25] and Alqahtani and Syed [26] demonstrated that Blockchain technology offers a secure, transparent, and tamper-resistant solution for digital evidence storage. As organizations continue to migrate critical systems and sensitive information to cloud platforms, the importance of cloud forensics is expected to increase significantly.

VI. Mobile Forensics

Mobile forensics is the extraction, analysis, and preservation of evidence from mobile devices such as smartphones, tablets, smartwatches, and portable communication devices. With the popularity of mobile devices, mobile forensics is a growth area in digital investigations.

Mobile devices hold lots of personal and organizational data, such as call logs, text messages, emails, multimedia files, GPS location data, application records, internet browsing history

Mobile forensic techniques are used to gain and obtain valuable evidence, as mobile devices are often used in criminal and cybercrime activities. The standard steps involved in the mobile forensics process are: Device Seizure, Evidence Preservation, Data Acquisition, Data Analysis, and Reporting. Forensic tools can recover deleted files, decrypt protected information, and analyse application artefacts.

But there are some difficulties with mobile forensics. Technological advances, a plethora of devices, encryption, operating system updates, and privacy laws are making evidence collection challenging. Moreover, cloud synchronization capabilities often necessitate investigators to study both mobile devices and associated cloud services at the same time. Forensic investigators need to stay current with advancements in mobile technology to meet new, ever-changing cybersecurity challenges.

VII. Cybersecurity Challenges in Digital Forensics

Digital forensic investigators face many challenges in the evolving nature of cyberattacks. It is an ongoing practice among cybercriminals to find new ways to evade detection, alter evidence, and exploit vulnerabilities in digital infrastructure. These issues, therefore, mean that the forensic investigator faces several technical, legal, and operational issues in the course of investigations (Fig. 3).

A. Large Volumes of Data

The vast amount of data generated by today's information systems is one of the largest challenges in digital forensics. Network devices, cloud platforms, mobile applications, and IoT devices constantly generate logs, packets, metadata, and user activity. Investigators have to be able to sift through huge amounts of information to find the evidence that counts, efficiently and accurately [14].

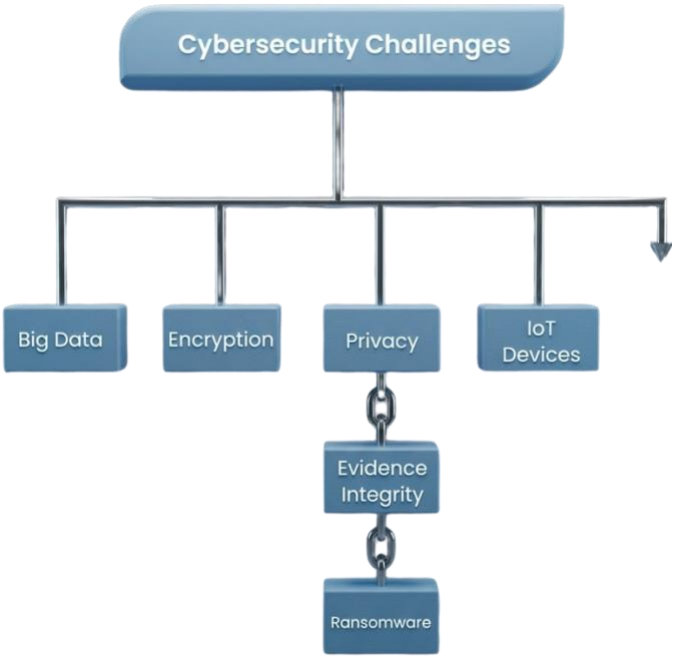

Fig. 3. Cybersecurity Challenges Affecting Digital Forensic Investigations

B. Encrypted Communications

Encryption technologies are widely adopted, protecting information while also making forensic investigations more difficult. Often, attackers use encrypted communication channels, virtual private networks (VPNs), and secure messaging apps to hide malicious activity. This poses challenges for investigators who may not have access to key evidence required for incident reconstruction [15].

C. Evidence Integrity and Preservation

Preserving the integrity of evidence is crucial to providing admissible digital evidence in legal proceedings. Investigators are required to adhere to proper procedures to ensure that evidence is not altered during collection, storage, and analysis. In computer investigations, blockchain is proposed as a means to enhance evidence integrity and traceability through blockchain-based forensic frameworks [15], [14].

D. Legal and Jurisdictional Issues

Cybercrimes often have international dimensions and pose legal issues regarding evidence gathering and prosecution. Each country has its own privacy rules, cyber protection laws, and evidence collection protocols. These differences make investigations in multinational organizations with distributed cloud infrastructures more complex [16].

E. Emerging Technologies

Advancements in Cloud computing, AI, machine learning, and the Internet of Things technologies have created new challenges for the collection, analysis, and preservation of digital evidence. Distributed architectures, virtualized environments, and autonomous systems are hard to investigate using traditional forensic tools [17].

VIII. Ransomware and Network Forensic Analysis

Ransomware is one of the most damaging forms of cybercrime. Modern ransomware attacks encrypt victims' data and demand ransom payments in exchange for decryption keys. The emergence of Ransomware-as-a-Service (RaaS) has made ransomware attacks more common and accessible, allowing cybercriminals to buy or lease ransomware tools without requiring advanced technical skills [18], [19].

Network forensics is an essential tool for ransomware investigations. Network traffic, communication patterns, and malicious connections enable investigators to identify the source of attacks and detect command-and-control (C2) communications associated with ransomware campaigns. Sharmila and Chaudhari [18] emphasized the importance of forensic analysis and cyber threat intelligence in improving ransomware detection. Similarly, Choo et al. [19] highlighted that threat intelligence platforms can help investigators detect malicious URLs and indicators of attack. Berrueta et al. [20] developed repositories and datasets to evaluate the effectiveness of ransomware detection mechanisms. These resources provide opportunities for researchers and security professionals to evaluate and improve forensic tools for combating emerging ransomware attacks.

Ransomware has become a highly profitable criminal business due to the growth of the RaaS ecosystem. The economic framework of ransomware operations on the darknet was explored by Meland et al. [21], while Greenstein [22] examined the impact of ransomware attacks on critical infrastructure sectors. The integration of forensic analysis, machine learning, and cyber threat intelligence is expected to improve ransomware detection and strengthen organizational resilience against future attacks [23].

IX. Internet of Things and Digital Forensics

The Internet of Things (IoT) is one of the most significant technological advancements of recent years. From healthcare and transportation to industrial automation, smart homes, critical infrastructure, and other applications, IoT devices are widely deployed across sectors. While the IoT technologies improve efficiency and connectivity, they also present significant cybersecurity risks [24]. The diversity of devices, limited computational resources, proprietary communication protocols, and distributed architecture make IoT forensic investigations very different from traditional forensic processes. A key challenge for investigators is collecting evidence from multiple interrelated devices while maintaining data integrity and complying with privacy laws.

Jindal et al. [17] argue that the volume of data generated in IoT environments is enormous, making forensic analysis more complex. Moreover, many IoT devices are not well equipped for logging, so there is less forensic evidence to be gathered. To overcome these problems, researchers have suggested blockchain-based forensic frameworks. Hossain et al. [25] proposed a blockchain-based method to save forensic evidence

in IoT systems. Likewise, Li et al. [27] presented privacy-preserving blockchain solutions for sharing secure evidence and ensuring traceability. AI is also becoming a key aspect of IoT security. Feng et al. [29] introduced deep reinforcement learning methods to optimize the security response, and Zhang et al. [31] discussed machine learning methods to enhance the reliability and security of the IoT system. However, many challenges remain regarding scalability, interoperability, privacy protection, and real-time forensic analysis.

X. Comparative Analysis of Existing Studies

The literature demonstrates substantial progress in digital forensic methodology in network, cloud, mobile, ransomware, and IoT areas. The first studies focused mainly on evidence collection [26] and on digital investigation frameworks [24]. Subsequent studies led to the development of intrusion detection and honeypot technologies, as well as network monitoring technologies [26], [27].

The latest studies have focused on ransomware detection, integration with cyber threat intelligence, evidence preservation using blockchain, and security mechanisms powered by artificial intelligence [1]. Selected studies suggest that Advancements in digital forensic solutions are becoming increasingly automated, machine learning-based, and dependent on blockchain technology and threat intelligence platforms. Yet, the currently available solutions still have various issues with scalability, architectural complexity, protection, and flexibility in the face of changing cyber threats. The following comparative table outlines the advantages and disadvantages of large-scale studies focused on network forensics, ransomware analysis, IoT security, blockchain-based evidence preservation, intrusion detection systems, and digital investigation processes.

XI. Future Research Directions

The studies included in the comparative analysis were selected based on their relevance to digital forensics, cybersecurity, ransomware investigation, cloud forensics, IoT security, and digital evidence preservation. The comparison was conducted using four evaluation criteria: the proposed method, the working model, the practical contribution, and the identified limitations. These criteria provide a consistent basis for evaluating the strengths and weaknesses of existing forensic approaches. Digital forensics research should continue to address the shortcomings of current methodologies and navigate the ever-changing technological landscape.

A. Artificial Intelligence for Forensic Automation

AI and machine learning can streamline evidence collection, anomaly detection, malware identification, and incident reconstruction. Future systems should include explainable artificial intelligence models that will give a clear forensic result [28],

B. Blockchain-Based Evidence Management

Blockchain technology has the potential to provide solutions for the integrity and transparency of evidence and for chain-of-custody management. The scalability and performance of blockchain should be explored in future research to facilitate large-scale forensic investigations [29].

C. Cloud-Native Forensic Frameworks

With the growing trend towards cloud computing, researchers will need to create forensic models tailored for distributed and virtualized environments. These frameworks should enable evidence collection, retention, and analysis of evidence in multi-cloud environments [30][33].

D. IoT Forensics

As more IoT devices are deployed, a lightweight forensic solution is needed that can operate in resource-constrained environments. In the future, there is a necessity to standardize IoT forensic processes and enhance the evidence collection ability [31-33].

E. Advanced Threat Intelligence Integration

Combining DF with threat intelligence platforms can enhance incident response and detection of cyber threats. Future systems should provide features for real-time intelligence sharing and automated attack correlation [7] [26]. Future research directions include forensic analysis of encrypted cloud environments, cross-jurisdictional digital evidence handling, privacy regulations (e.g., GDPR and data protection requirements), and the scalability of AI-assisted forensic systems.

The comparative analysis indicates that recent research has shifted from conventional evidence-collection techniques toward intelligent forensic frameworks that incorporate blockchain, machine learning, and cyber threat intelligence. Although these approaches improve detection accuracy and evidence integrity, they often introduce higher computational complexity, scalability challenges, and implementation costs. Furthermore, many proposed solutions have been evaluated in controlled environments and require additional validation in large-scale real-world deployments. These limitations highlight the need for more adaptive, scalable, and interoperable digital forensic solutions to address emerging cyber threats.

XII. Conclusion

Digital forensics has become a vital part of modern cybersecurity. The growing sophistication and prevalence of cyber threats demand sophisticated forensic tools to help organisations conduct cyber incident investigations, determine who is behind the attackers, and retain evidence and facilitate legal action. This review paper aims to compare and contrast digital forensics with its key areas, such as network, cloud, and mobile forensics. Network forensics is crucial for analyzing traffic and investigating cyberattacks. Cloud forensics is used to deal with the specific issues of distributed and virtualized computing environments, and mobile forensics is concerned with finding evidence on mobile phones and portable devices. Emerging challenges covered ransomware attacks, IoT environments, blockchain integration, AI, and cyber threat intelligence were also discussed in the paper.

The literature indicates that digital forensics remains a rapidly evolving field, adapting to emerging technologies and advanced cyberattacks. While substantial strides have been made, issues of data volume, evidence integrity, privacy protection, scalability, and legal compliance remain unaddressed. Research and development efforts should incorporate AI, blockchain technologies, and cloud-native forensic processes and systems, alongside advanced threat intelligence, to enhance the effectiveness of digital investigations and cybersecurity measures.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, S.K., W.A., I.A.S., and B.G.; methodology, S.K., W.A., and B.G.; validation, I.A.S.; writing—original draft preparation, S.K., W.A., B.G.; writing—review and editing, I.A.S., and B.G.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] W. Mazurczyk, K. Szczypiorski, and H. Tian, “Network forensics and challenges for cybersecurity,” Annals of Telecommunications, vol. 69, pp. 345–346, 2014.

[2] A. Almulhem, "Network forensics: Notions and challenges," 2009 International Conference on CyberWorlds, Bradford, UK, 2009, pp. 313-317.

[3] W. G. Kruse, Computer Forensics: Incident Response Essentials. Addison-Wesley, 2001.

[4] B. Carrier and E. H. Spafford, “Getting physical with the digital investigation process,” International Journal of Digital Evidence, vol. 2, no. 2, 2003.

[5] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," Proceedings of the Digital Forensic Research Workshop (DFRWS 2004), Baltimore, Maryland, USA, 2004, pp. 1-9.

[6] R. Filasiak, M. Grzenda, M. Luckner, and P. Zawistowski, “On the testing of network cyber threat detection methods on spam example,” Annals of Telecommunications, vol. 69, no. 5-6, pp. 261–271, 2014.

[7] B.-C. Cheng, G.-T. Liao, H.-C. Huang, and P.-H. Hsu, “CHEETAH: A space-efficient HNB-based NFAT approach to supporting network forensics,” Annals of Telecommunications, vol. 69, no. 5-6, pp. 287–299, 2014.

[8] T.-Y. Wu, T.-T. Tsai y Y.-M. Tseng, “Efficient searchable ID-based encryption with a designated server,” Annals of Telecommunications, vol. 69, no. 5-6, pp. 301–314, 2014.

[9] S. Wendzel and J. Keller, “Hidden and Under Control: A survey and outlook on covert channel-internal control protocols,” Annals of Telecommunications, vol. 69, no. 5-6, pp. 315–327, 2014.

[10] Li F, Zhang X, Yu J, Shen W. Adaptive JPEG steganography with new distortion function. Annals of Telecommunications 2014; 69(7): 431-440. DOI: 10.1007/s12243-013-0415-2.

[11] A. C. Castillo, “Network forensics: Concepts and challenges,” Journal of Forensic Sciences & Criminal Investigation, vol. 13, no. 1,555853. DOI: 10.19080/JFSCI.2019.13.555853 2019.

[12] D. Brezinski and T. Killalea, “Guidelines for evidence collection and archiving,” RFC 3227, BCP 55, 2002.

[13] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

[14] Watson, S., & Dehghantanha, A. (2016). Digital forensics: The missing piece of the Internet of Things promise. Computer Fraud Security, 2016, 5–8.

[15] B. Scottberg, W. Yurcik, and D. Doss, “Internet honeypots: Protection or entrapment?” IEEE International Symposium on Technology and Society, 2002.

[16] L. Spitzner, The Honeynet Project, 2007.

[17] NetWitness, “Network forensics in cybersecurity: Unveiling the invisible adversary,” Oct. 2025.

[18] S. P. Sharmila and N. S. Chaudhari, “Conceptual study of prevalent methods for cyber-attack prediction,” in Expert Clouds and Applications, Springer, pp. 631–641, 2022.

[19] E. Choo, M. Nabeel, D. Kim, R. De Silva, T. Yu, and I. Khalil, “A large-scale study and classification of VirusTotal reports on phishing and malware URLs,” Proceedings of the ACM on Measurement and Analysis of Computing Systems, vol. 7, no. 3, pp. 1–26, 2023.

[20] E. Berrueta, D. Morato, E. Magaña, and M. Izal, “Open repository for the evaluation of ransomware detection tools,” IEEE Access, vol. 8, pp. 65658–65669, 2020.

[21] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, “The ransomware-as-a-service economy within the darknet,” Computers & Security, vol. 92, 101762, 2020.

[22] B. Greenstein, “The impact of Ransomware-as-a-Service on critical infrastructure,” Doctoral dissertation, Utica University, 2022.

[23] B. Payne and E. Mienie, “Multiple-extortion ransomware: The case for active cyber threat intelligence,” ECCWS 2021, 2021.

[24] A. Jindal, N. Kumar, and M. Singh, "Future scope and challenges of Internet of Things technologies," Journal of Network and Computer Applications, vol. 212, p. 103560, 2023.

[25] M. Hossain et al., "Blockchain-based framework for evidence collection and preservation in IoT networks," IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6842–6855, 2023.

[26] F. Alqahtani and R. Syed, “Blockchain-integrated forensic framework for evidence preservation and transparency in IoT environments,” 2023.

[27] Y. Li et al., “Privacy-preserving blockchain scheme for secure information sharing and traceability in IoT systems,” 2023.

[28] F. U. Islam, G. Liu, W. Liu, and Q. M. U. Haq, “A deep learning-based framework to identify and characterise heterogeneous secure network traffic,” IET Information Security, vol. 17, no. 2, pp. 294–308, 2023.

[29] X. Feng et al., “Deep reinforcement learning-based security defense strategy for IoT networks,” 2023.

[30] Y. Zhang et al., “Security and reliability challenges in machine learning-based IoT systems,” 2023.

[31] P. N. Tan, M. Steinbach, and V. Kumar, Introduction to Data Mining. Addison-Wesley, 2005.

[32] A. Sumra, I. Ahmad, H. Hasbullah and J. -l. bin Ab Manan, "Classes of attacks in VANET," *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, Riyadh, Saudi Arabia, 2011, pp. 1-5,

[33] I. A. Sumra, H. Hasbullah and J. -l. A. Manan, "VANET security research and development ecosystem," *2011 National Postgraduate Conference*, Perak, Malaysia, 2011, pp. 1-4, doi: 10.1109/NatPC.2011.6136344.

TABLE I: Comparative Analysis of Existing Studies in Digital Forensics and Cybersecurity

Author Name	Proposed Method	Working of the Model	Limitation
Mazurczyk, Szczypiorski, & Tian (2014) [1]	Network forensics framework for cybersecurity investigations	Collects network traffic data Analyzes and preserves digital evidence Supports cybercrime investigations and threat identification	Large volumes of network data Time-consuming evidence analysis
Filasiak, Grzenda, Luckner, & Zawistowski (2014) [6]	Realistic network threat testing datasets	Creates realistic datasets for spam and cyber threat detection Evaluates detection accuracy and performance	Results depend on dataset quality Limited adaptability to new threats
Cheng, Liao, Huang, & Hsu (2014) [7]	CHEETAH space-efficient NFAT approach	Uses advanced classifiers for attack analysis Reduces storage requirements in forensic systems	Requires classifier training Computational sophistication
Wendzel & Keller (2014) [9]	Covert channel micro-protocol analysis	Categorizes covert communication protocols Improves hidden channel analysis and optimization	Hidden channels remain difficult to detect Real-time monitoring challenges
Sharmila, Tiwari & Chaudhari (2026) [18]	Network forensic analysis integrated with VirusTotal	Captures ransomware traffic Classifies packets as malicious, suspicious, or benign Validates findings using VirusTotal	Dependency on VirusTotal API Limited ransomware sample availability
Meland, Bayoumy & Sindre (2020) [21]	RaaS economy analysis	Studies Ransomware-as-a-Service ecosystem Examines attacker business models and operations	Focuses on economic aspects Limited technical detection methods
Berrueta et al. (2020) [20]	Ransomware detection evaluation repository	Provides datasets and testing environments Supports evaluation of ransomware detection tools	Less effective against new ransomware variants
Islam et al. (2023) [28]	Deep learning-based network traffic classification	Uses deep learning models Classifies malicious and legitimate traffic patterns	Requires large datasets High computational cost
Hossain et al. (2023) [25]	Blockchain-based evidence preservation framework	Stores forensic evidence on blockchain Ensures integrity, confidentiality, and availability	Blockchain scalability issues High processing overhead
Alqahtani & Syed (2023)[26]	Blockchain-integrated forensic framework	Uses smart contracts and blockchain APIs Maintains immutable forensic records	Complex implementation High deployment cost

Feng et al. (2023) [29]	Deep Reinforcement Learning Security Model (SDSA)	Optimizes security resource allocation Uses multi-agent reinforcement learning	Extensive training requirements Computationally expensive
Zhang et al. (2023) [30]	Machine Learning-based IoT security framework	Detects adversarial attacks Improves IoT security reliability	Effective mainly for known attacks Limited against zero-day threats
Almulhem (2009) [2]	Network Forensics Framework	Collects and correlates network evidence Supports cyberattack investigation and documentation	Complex evidence management Large-scale data collection challenges
Carrier & Spafford (2003)[4]	Integrated Digital Investigation Process (IDIP)	Uses readiness, deployment, investigation, and review phases Provides structured forensic methodology	Time-consuming process Requires trained investigators
Lunt (1993) [13]	Intrusion Detection System (IDS)	Detects attacks using signature-based methods Uses anomaly-based monitoring for suspicious behavior	False positives and negatives Limited forensic information
Spitzner (2007) [16]	Honeynet/Honeypot Framework	Attracts attackers into controlled environments Collects attack evidence and behavior patterns	Legal and ethical concerns Potential entrapment issues