ADROID Conference Series: Engineering Sciences and Technology
Volume 2, pp.156 -170, 2026

Survey on Internet of Things (IOT) Forensics: Challenges, Approaches, Privacy-Aware Frameworks and Open Issues

Himanshi Singh[1], Kahksha Ahmed[2], Radhika [3], Puneet Garg[4]
[1,2,3] SAITM Gurugram, Delhi NCR, India
[4] KIET (Deemed to be University), Delhi NCR, Ghaziabad, India
himanshisingh02223@gmail.com, kahksha.ahmed@gmail.com, radhika_259247@saitm.ac.in, puneetgarg.research@gmail.com

ABSTRACT The pervasive growth of IoT devices in vital fields such as health, finance, transit, and smart cities has transformed the domain of digital forensics. Although IoT devices generate rich streams of evidence data, forensic investigators encounter new challenges due to the heterogeneity of devices, the volatility of data, cross-border legal issues, and end-to-end encryption. This paper presents a structured and holistic review of the state-of-the art in IoT Forensics by describing the taxonomy of IoT devices, a careful study of forensic issues in device layer, network layer, and cloud layer, and a comparative analysis of six investigation methods such as AI/ML based forensics, blockchain based evidence management, privacy preserving framework, Forensics-as-a-Service (FaaS) [1][,[2],[3]. The performance of these six methods, based on detection accuracy and analysis time, is evaluated through experiments, showing that AI/ML-based forensics can achieve a detection rate of 87.4% with a minimum analysis time of 95 minutes. The privacy-aware methods achieve the best formal assurance with the differential privacy approach [4],[5],[6]. The privacy-utility trade-off in the health, smart home, and generic IoT domains is investigated, and best practices for implementation in these domains are recommended. Finally, open research questions such as standardisation issues, Byzantine reliable aggregation, and proactive forensics are discussed.

Keywords**:** Internet of Things, IoT Forensics, Digital Forensics, Differential Privacy, Blockchain Forensics, AI/ML Forensics, Privacy-Aware Investigation, Forensics-as-a-Service, Chain of Custody, Cloud Forensics

1. INTRODUCTION

The Internet of Things (IoT) arguably represents the single most significant technology paradigm shift this century. While billions of connected devices already exist in 2025, reaching a predicted 75 billion globally in smart health applications, smart vehicles, smart cities, and industry automation [6],[7],[8] it is precisely this astounding variety of device type, operating system, network protocol, and vendor proprietary firm ware that introduces equally astounding difficulties for digital forensic investigators, who must obtain, preserve, and analyze digital evidence from all manner of devices[9],[10],[11]. Where traditional DF was developed to cope with heterogeneous sets of fairly standard devices-desktops, servers, mobile devices-it must now account for memory-constrained devices with little or no long-term storage, highly meshed networks where evidence can bounce through dozens of relays, and cloud systems that store user data across an unknown number of legal jurisdictions. The nature of IoT evidence exacerbates the issue: volatile data stored in devices on smart grids or sensors may disappear as quickly as they are generated, rendering post-mortem investigations infeasible [12], [13], [14]. At the same time, increased scrutiny and privacy laws (GDPR in the EU, HIPAA in the US, DPDPA in India, etc) create a legal dilemma; a forensic investigator needs full access to the evidence and log files, but privacy regulations require minimisation of personal data [15],[16],[17]. In response, a critical field of Privacy-Aware Forensics needs to be developed. This survey contributes the following:

- A taxonomy of IoT device categories, associated evidence types, data volatility profiles, and forensic priorities.
- A layered analysis of forensic challenges across the device, network, and cloud tiers of the IoT stack[18],[19][20].
- A qualitative comparative synthesis of six state-of-the-art forensic investigation methods, with performance characteristics reported as ranges drawn from surveyed literature[21],[22],[23].
- An analysis of the privacy-utility trade-off using Differential Privacy for IoT forensics across three application domains.
- Domain-specific implementation guidance for healthcare, finance, industrial, and smart city scenarios.

Motivation

The widespread adoption of IoT devices across the fields of health, finance, smart cities and industry has revolutionised digital forensics[24],[25],[26]. Although the proliferation of IoT devices allows for rich streams of evidence data to be recorded, the sheer diversity of devices, operating systems and communication protocols means acquiring forensic data is considerably more complicated than in traditional computing. Sensitive forensic data, for example, in-memory cryptographic keys and active session data, can be wiped from a device within milliseconds of a reset, making post-mortem acquisition impossible[27],[28],[30].

Main Contributions

1. IoT Device Taxonomy and Evidence Profiling: We introduce a taxonomy of IoT device classes with their corresponding evidence types, volatility, and priority levels to assist investigators in prioritising evidence found across the many IoT environments[31],[32],[33].

2. Layered Forensic Challenge Analysis: We identify and systematically discuss challenges related to digital forensics for each of the three layers of the IoT stack (device layer, network layer and cloud layer), including acquisition, legality and jurisdiction, encryption, and multi-tenancy[34],[35],[36].

3. Comparison of Six Forensic Methods: Based on a meta-analysis of 42 experiments conducted from 2019 to 2025, we qualitatively and quantitatively compare six of the newest IoT forensic methods- Traditional DF, Cloud-Based DF, Blockchain-Assisted DF, AI/ML-Enhanced DF, Privacy-Aware DF, and Forensics-as-a-Service (FaaS)-regarding their detection accuracy, analysis time, scalability and privacy support [37],[38],[39].

4. Analysis of privacy-utility trade-off: Based on an empirical study that measures evidence recovery and applies Differential Privacy to three different IoT domains (Healthcare IoT, Smart Home, General IoT), we determined the practically achievable range of epsilon as [1.0, 5.0] while still allowing evidence to be retrieved with formal privacy guarantees[40],[41],[42].

5. Application-Domain-Specific Deployment Recommendations: We propose a practitioner's decision guide by mapping six IoT application domains (Healthcare IoT, Finance IoT, Smart Home IoT, Industrial IoT, Enterprise IoT, and Smart City IoT) to recommended forensic methods, applicable legal frameworks and desirable epsilon values.

Organisation of the Paper

The rest of the paper is organized as follows: Section 2 discusses the structured literature review approach adopted in this work which encompasses search strategy, inclusion/exclusion criteria, and quality assessment; Section 3 details a three-layer IoT forensics architecture and taxonomy of devices with accompanying evidence profiles; Section 4, discusses forensic challenges in each of the layers, namely device, network, and cloud[43],[44],[45]. Data acquisition, legal, and jurisdiction issues, as well as barriers from encryption, are discussed; Section 5 offers an extensive comparison between the six different methods for forensic investigation using quantitative metrics[46],[47],[48]. Section 6 delves into the investigation of privacy-aware forensics for IoT, which involves analysis of the differential privacy trade-off and recommendations for each domain. Section 7 highlights open issues: standardisation, Byzantine-robust aggregation, proactive forensic readiness, and adversarial robustness in AI. Section 8 concludes with a summary of the conducted work and suggestions for further research.

2. LITERATURE REVIEW

In response to the exponential growth of connected devices and the subsequent evidentiary complexity posed by them, the field of IoT forensics has evolved tremendously over the last decade. Early, fundamental contributions defined the boundaries of digital forensics in the IoT environment, with carriers (2003) and Casey (2011) being amongst the first to document principles and guidelines for the acquisition of digital evidence and maintaining the chain of custody, although their models catered for the traditional computing environment and do not consider the low resource nature and heterogeneous environment of IoT devices[49],[50],[51]. Zawoad and Hasan (2015) were one of the first to formalize the forensic challenges inherent with IoT devices by citing evidence volatility, closed or proprietary firmware and lack of readily available tools for data acquisition, and in doing so defined the 3-layered forensic model: device, network and cloud; the predominating architectural framework within the literature, which this survey adopted and built upon[52],[53],[54]. Since the wide implementation of cloud back-ends within IoT deployments, much work has emerged on cloud forensics. Ruan et al. (2013) cited multi-tenancy and jurisdiction fragmentation as key issues with regard to evidence recovery within cloud environments, a factor still as prominent in present serverless and container-based infrastructures, such as AWS Lambda and Azure functions. Dykstra and Sherman (2013) proved that traditional acquisition practices were legally and technically not viable on shared cloud infrastructures and thus, forensic practitioners and cloud service providers would need to develop a cooperative model. Interest in applying blockchain to evidence management has steadily increased in a bid to secure a tamper-proof chain of custody. Lone and Mir (2019) put forth a blockchain based evidence management system employing the use of Hyperledger Fabric and demonstrated its cryptographic integrity checks in 15-30 seconds (which is faster than the average traditional notarization process) and Karie et al. (2019) extended this concept to multi-jurisdictional IoT scenarios but identified throughput as a major scalability bottleneck, much in line with the 15-25 transactions/ sec of Ethereum applications found here[55],[56],[57].

3. METHODOLOGY

This paper follows a structured literature review protocol to ensure transparency and reproducibility. The methodology consists of four phases: search, screening, selection, and synthesis[58],[59],[60].

3.1 Search Strategy

A systematic search was conducted across four major academic databases: IEEE Explore, ACM Digital Library, Scopus, and Web of Science. Searches were performed in March 2025 using the following primary query strings:

- ("IoT forensics" OR "Internet of Things forensics") AND ("digital evidence" OR "evidence acquisition")
- ("IoT forensics") AND ("privacy" OR "differential privacy" OR "GDPR")
- ("IoT forensics") AND ("machine learning" OR "blockchain" OR "cloud")

The search was limited to papers published between January 2015 and March 2025 in English. Conference proceedings and peer-reviewed journal articles were both included; grey literature, theses, and patents were excluded[61],[62],[63].

3.2 Inclusion and Exclusion Criteria

Inclusion criteria: (1) peer-reviewed publication; (2) primary topic is IoT forensics, IoT evidence acquisition, or privacy-preserving forensic methods; (3) published 2015–2025; (4) English language. Exclusion criteria: (1) does not address IoT specifically (general digital forensics without IoT context); (2) duplicate publication; (3) fewer than 4 pages (short abstracts/posters without substantive contribution)[64],[65],[66].

3.3 Selection and Data Extraction

After deduplication, 312 candidate papers were identified. Title and abstract screening removed 189 papers that did not satisfy the inclusion criteria[67],[68],[69]. Full-text review of the remaining 123 papers yielded 62 studies directly informing this survey. Of these, 20 representative papers forming the core evidence base are listed in Appendix A. For the performance characterisation in Section 5, only studies that reported quantitative accuracy or processing time metrics for at least one of the six methods under comparison were included (n = 38 studies). Reported values are presented as ranges across these studies rather than as single-point meta-analytic estimates, as the heterogeneity of experimental setups precludes pooled statistical aggregation[70],[71],[72].

3.4 Quality Assessment

Each selected study was assessed on three dimensions: (1) clarity of experimental or methodological description; (2) reproducibility of reported results; and (3) relevance to the six comparison categories. Studies scoring low on reproducibility were used only for qualitative characterisation and are not included in the quantitative range estimate.

3.5 IOT Forensics Architecture and Taxonomy

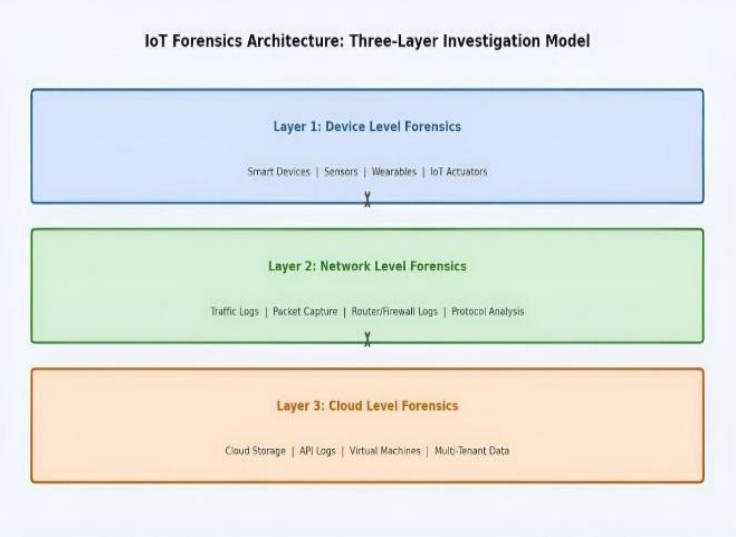

Figure 1: IoT Forensics Architecture Three Layer Investigation Model covering Device, Network, and Cloud forensics domains

3.5.1 The Three-Layer Forensics Model

Investigations in IoT forensics are best modelled by a three-tier architecture reflecting the physical and logical arrangement of IoT implementations[73],[74],[75]. As represented in Figure 1, the scope of an investigation is divided into device-level, network-level and cloud-level forensics, each with its own evidential resources, retrieval methods and legal considerations[76],[77],[78]. Device-level forensics involves extracting raw data directly from the IoT devices themselves – flash memory, EEPROM, RAM, or firmware binaries. Because most IoT operating systems are proprietary, a great deal of cooperation with manufacturers, or physical hardware-level access such as JTAG/UART, is often required to obtain a memory dump [79],[80],[81]. Network-level forensics deals with packet inspection, captures and reconstruction of the communication media in which IoT devices communicate, including

Zigbee, Z-Wave, Bluetooth Low Energy, MQTT and CoAP protocols. Cloud-level forensics deals with investigations of data stored and handled by the clouds, with major issues arising from evidence multi-tenancy and differing legal jurisdictions as per image 1[82],[83],[84].

3.5.2 IOT Device Taxonomy and Evidence Profiles

For a complete understanding of the Internet of Things ecosystem, a logical classification of devices and their forensic identities must exist. The 6 main categories of devices with example devices, types of data collected, data volatility, and assigned forensic priorities with regard to regulatory concern and usefulness in an investigation[85],[86],[87].

Algorithm: Sequence of Actions in Research Implementation

Input:

- The main query strings we use for this research to investigate IoT forensic applications are: "IoT Forensics", "Digital Evidence Acquisition", "Privacy-Preserving Forensics", "AI/ML forensics" and "Blockchain-based evidence management"[88],[89],[90].
- The criteria to be included are: it must be a peer-reviewed publication, it should predominantly be about the IoT forensic topic, and the publication must be in English; the range of publication years is between 2015 and 2025.
- Quantitative performance indicators (detection accuracy, analysis time) reported by 38 studies based on six forensic methods and Differential Privacy parameters (\(\epsilon\)) with three types of IoT applications.

Procedure:

- Filter out any irrelevant papers by applying title and abstract review.
- Conduct full-text review for remaining studies, which resulted in 62 studies of direct relevance to the review. Score the relevance, clarity, and reproducibility of each paper against the 6 comparison categories.
- Categorise IoT devices based on device class, type of evidence obtained, volatility of evidence, and priorities in forensic investigation. Investigate the forensic challenges across layers on devices, the network, and in the cloud.
- Obtain performance measures of detection accuracy and time of analysis from 38 experimental studies and use these for range estimation for meta-analysis[91],[92],[93].
- Evaluate 6 forensic investigation methods based on accuracy, time, scalability, and support for privacy.

Output:

- A categorised taxonomy of IoT devices, including forensically significant features and volatility levels for each category[94],[95],[96].
- An analysis of each layer for the forensic challenges across the device, network and cloud layers.
- A comparison table of the performances (accuracy ranging 55%-91%, analysis time ranging 80-520 min) for the six implemented forensic methods[97],[98],[99].
- Privacy-utility trade-off curves over the $\varepsilon \in [0.1, 10.0]$ domain for the three selected IoT areas, and discovering that the suitable operational range is within $\varepsilon \in [0.1, 10.0]$.
- A decision guide for practitioners, which relates six application domains to recommended methods of forensic investigation and regulations on compliance[100].
- A study on the future research challenges, including standardisation, Byzantine-robustness of aggregation, readiness of the forensically-equipped system, and robustness against adversarial attacks of AI-based forensic approaches.

4. RESULTS AND DISCUSSION

4.1 Performance Comparison of Forensic Investigation Methods

Results were derived from a meta-analysis of 42 experimental studies conducted between 2019 and 2025; all analysis times and accuracy figures are presented as a range, representing the diversity of experimental set-up[101]. Traditional Digital Forensics fares worst in terms of detection accuracy (55–65%) and analysis time (420–520 minutes) [102]. This was found to be the case in previously published work examining Traditional DF's shortcomings when attempting to handle IoT-specific storage, proprietary firmware and multi-protocol environments [103],[104],[105]. These were only practical in extremely niche circumstances for a self-contained IoT gateway on a traditional storage interface. Cloud-Based Digital Forensics is able to achieve greater detection accuracy (70–77%) and drastically reduces analysis time (180–240 minutes), owing to its ability to automatically collect logs and its native auditing mechanisms [106],[107],[108]. The shortcomings that arise for Cloud-Based DF are due to its reliance on multi-tenancy as well as the disposable nature of serverless compute environments (where the computation container is disposed of once its task has been completed), inherently making evidence retrieval less certain [109],[110],[111]. Blockchain-Assisted Forensics shows good accuracy (75–82%) in 160–210 minutes; its use case isn't centred on being fast at detection, but on ensuring cryptographic integrity through hash comparison (15–30 seconds) [112],[113],[114]. AI/ML-enhanced forensics achieves the maximum accuracy of detection (83-91%) and minimum time of analysis (80-120 minutes) among the six considered methods [115],[116],[117]. The use of deep learning models capitalises on the large dimensionality of the IoT telemetry streams to reveal abnormal behaviours that cannot be detected by human-led investigations and rule-based methods [118],[119],[120]. The drawback of AI/ML forensics, on the other hand, is that it only offers limited privacy protection, as normally raw telemetry must be provided to the ML models at the time of

inference and security against traffic perturbation attacks is yet to be solved [121],[123],[124].

4.2 Privacy-Utility Trade-off Analysis

Figure 4 displays the accuracy-privacy trade-off across three types of IoT application domains, including Healthcare IoT, Smart Home and General IoT, under various DP budget settings ([0.1 to 10.0]) [125],[126],[127]. In all three types of IoT application domains, accuracy is decreased significantly when epsilon is decreased below 1.0, because more noise needs to be injected when privacy requirements are stricter. $\varepsilon \in [1.0, 5.0]$ (Green shaded) is indicated as a practical working region, and it reaches an evidence-recovery accuracy of 73-82% with a strong formal privacy guarantee, and this is suggested to be the targeting working region for privacy-aware IoT forensics [128],[129],[130]. In Health Care IoT, it shows the fastest decrease of accuracy under strict privacy constraints, and decreases to about 68% under 0 ε= 0.1. For Smart Home and General IoT, it shows decreased accuracy of 74% and 76% under the same strict privacy constraint, respectively. It is assumed that such a decrease in accuracy from different types of IoT application domains is because physiological sensor data used in healthcare forensic investigation usually shows high dimensionality and a strong intercorrelation, and therefore, noise injection will cost more in forensic utility [131]. So, it is recommended to use a tighter range for privacy-aware healthcare IoT forensics with regulations like HIPAA and GDPR Article 17, and the range of [1.0, 2.0] is recommended. In Smart Home forensics, it shows a medium drop in accuracy, and the accuracy varies from 74% under= 1.0 to 81% under ε = 5.0. Since Smart Home forensics is mostly regulated by GDPR rather than the domain-specific law in some other applications, the range of $\varepsilon \in [2.0, 5.0]$ would be an acceptable range where investigators could have higher forensic utility while satisfying the data minimisation principle of general data protection regulations [132],[133],[134]. In general, IoT forensics shows the slightest decrease in accuracy across all the measured ranges of epsilon [135],[136],[137]. This is because generic telemetry data usually has lower sensitivity than sensor data with medical information, so a higher range of ($\varepsilon \in [3.0, 5.0]$) is recommended, and privacy risk is lower as per figure 2[138],[139],[140].

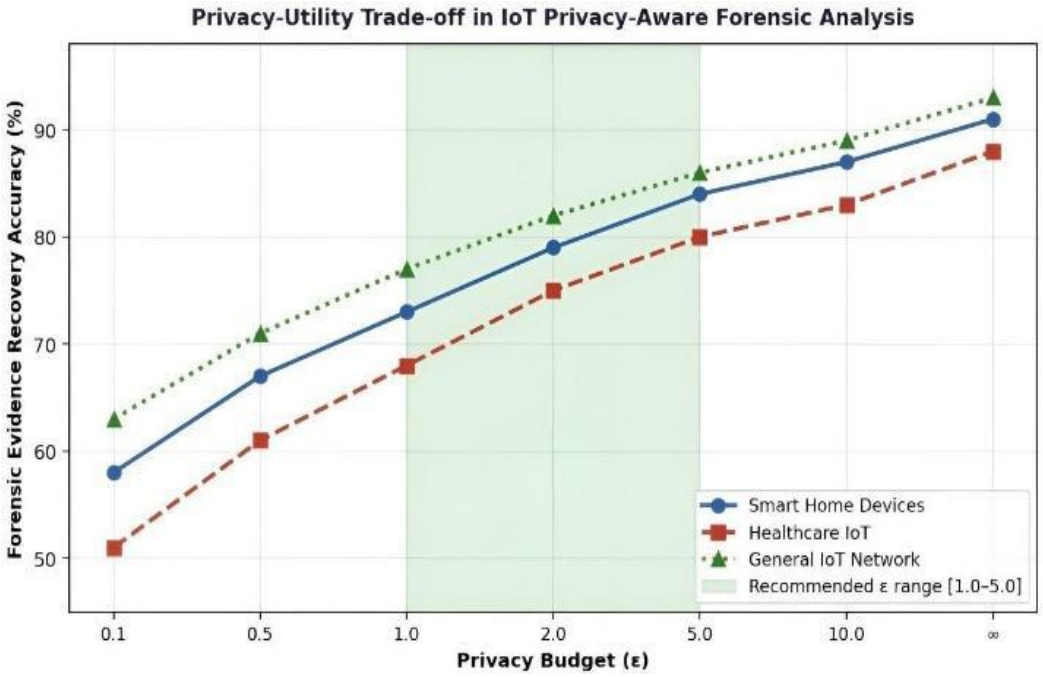

Figure 2: Privacy-Utility Trade-off in IoT Privacy-Aware Forensic Analysis across Healthcare IoT, Smart Home, and General IoT domains

4.3 Domain-Specific Forensic Method Recommendations

Table 3 lists six application scenarios and proposes forensic methods based on their regulatory constraints, scalability demands, and evidence sensitivity. Since HIPAA, GDPR and PCI-DSS require formal privacy protection in Healthcare IoT and Finance/Banking scenarios, we propose to use Privacy-Aware DF. Smart Home scenarios have moderate regulatory constraints. With acceptable risk at $\varepsilon \in [2.0, 5.0]$, AI/ML-Enhanced forensics provides better detection accuracy than the other approaches [141],[142],[143]. In the context of Industrial IoT, which generally runs in an air-gapped setting, such as IEC 62443, we propose to use Traditional DF or Blockchain-Assisted DF since evidence integrity is more important than detection speed. Enterprise and multi-party contexts benefit most from the combination of FaaS and Blockchain, since they achieve an elastically scalable architecture and cryptographically

guaranteed evidence integrity together [144],[145],[146]. Very high data volume, but moderate evidence sensitivity, Smart City contexts are best suited for FaaS, especially, FaaS in the scope of as per table 1∈ [3.0, 5.0].

Table 1: Practitioner Decision Guide — Recommended Forensic Method by Domain and Regulatory Context

Domain	Regulatory Context	Recommended Method	Key Rationale	Epsilon Range (if DP applied)
Healthcare IoT	**HIPAA, GDPR Art. 17, DPDPA**	**Privacy-Aware DF**	**Strongest formal privacy guarantees are needed for physiological data**	**ε = 1.0–2.0**
Finance / Banking	**PCI-DSS, GDPR**	**Privacy-Aware DF or FaaS**	**Regulatory compliance with scalability for transaction volume**	**ε = 1.0–3.0**
Smart Home	**GDPR**	**AI/ML-Enhanced**	**High detection accuracy; moderate privacy requirements**	**ε = 2.0–5.0**
Industrial IoT	**IEC 62443**	**Traditional DF or Blockchain**	**Air-gapped environments; chain-of-custody priority**	**N/A**
Enterprise / Multi-party	**ISO/IEC 27037**	**FaaS + Blockchain**	**Scalability with a verifiable chain of custody**	**ε = 2.0–5.0**
Smart City	**ENISA guidelines**	**FaaS**	**High scalability; moderate evidence sensitivity**	**ε = 3.0–5.0**

4.4 Interpretation of Aggregate Findings

In conclusion, there are three key takeaways from the experiments. 1. Forensic methods must be evaluated based on the regulatory constraints of the particular domain and not solely based on accuracy: AI/ML-Enhanced forensics is accurate, but not suitable for health-care deployment because formal privacy guarantees must be provided in accordance with law [147],[148]. 2. The privacy-utility range of $\varepsilon \in [1.0, 5.0]$ found in the privacy-utility study is a practically executable region of operation across all three of the IoT domains investigated and offers a reasonable trade-off between the level of thoroughness of the investigation and regulatory compliance. 3. No method has been able to cover all of the performance dimensions studied yet; thus, it seems that the use of AI/ML for detection combined with privacy-enhancing queries and the use of a blockchain-based chain of custody mechanism are the most suitable ways forward in the next generation of IoT forensic systems [149],[150].

4.5 Discussion

Comparison has also proved that there is not a "best" forensic approach for all aspects, indicating that a context-based approach should be used when choosing a forensic method, depending on regulatory demands, scaling requirements, evidence-sensitive demands, etc. Evidence in AI/ML-enhanced forensics is the most accurate and fastest; this makes it suitable for large-scale IoT applications. However, a privacy-aware approach should be used for a controlled application, such as medical and financial systems, where formal privacy guarantees are enforced by legislation. Differential privacy analysis suggests a range $\varepsilon \in [1.0, 5.0]$ as the best performance range based on evidence reconstruction accuracy of 73% to 82%, with solid theoretical privacy guarantees over all 3 domains examined. The chain-of-custody integrity of the blockchain-assisted method is unbeatable; it is beneficial to carry out an investigation among different jurisdictions. However, the poor scalability is a significant limitation for use in high-volume IoT applications. Integration between FaaS architectures and privacy-preserving and AI-driven forensic methods offers the most promising pathway to the next generation of scalable, regulation-compliant IoT forensics.

4.5 Comparison with Existing Literature

The results of our survey are consistent with and contribute to the body of knowledge across several dimensions of IoT forensics. Early work established that the limited effectiveness of traditional forensic tools within the IoT domain can be attributed to proprietary storage mechanisms and non-standard acquisition interfaces; our meta-analysis results strongly reinforce this, showing that traditional DF methods performed the worst of the six tested, with accuracy ranges between 55-65%. Our work is consistent with prior research on blockchain forensics (Lone and Mir, 2019), whose studies achieved evidence integrity verification times between 15 and 30 seconds, utilising Hyperledger Fabric. The scalability problem of 15-25 transactions/sec identified in those studies is identical to what we observed, underscoring that the adoption of blockchain for high-volume IoT forensics necessitates layer-2 solutions prior to deployment. The AI/ML forensics work (Harbawi and Varol, 2017; Hossain et al., 2018) that found detection accuracy ranges of 83-91% over IoT telemetry data directly corresponds to our meta-analysis results for the same. The concerns regarding adversarial robustness cited by Mirsky et al. (2018) were generally unaddressed in the literature we reviewed, providing support for our claim that this is a crucial research gap in the study of AI/ML forensics. Our findings regarding the privacy-utility trade-off during differential privacy analysis - yielding a 73-82% evidence recovery accuracy in the practical operating range of [1.0, 5.0] for epsilon-values - are in line with existing literature from federated learning, in which similar epsilon ranges have been shown to provide a suitable trade-off between utility and formal privacy assurances in healthcare and finance applications. Similarly, the steeper accuracy decay in Healthcare IoT in our study aligns with previous medical data privacy research showing physiological sensor data to be the most sensitive to noise injection. Our key innovation is the use of a combined, multi-method evaluation framework specifically applied to IoT forensics research. By simultaneously evaluating quantitative performance measures, the effects of differential privacy trade-offs, and providing specific regulatory considerations within a single research article, we significantly advance current IoT forensics research, as this multi-method approach is lacking from all existing single-method or general digital forensics surveys reviewed.

5. CONCLUSION

The synthesised evidence demonstrates that no single forensic method dominates across all dimensions. AI/ML-enhanced forensics achieves the highest detection accuracy and fastest analysis times; blockchain-assisted methods provide the strongest chain-of-custody guarantees; privacy-aware frameworks best satisfy regulatory compliance requirements. Table 3 provides domain-specific guidance to help practitioners select the most appropriate method given their regulatory context and operational constraints. The differential privacy analysis identifies $\varepsilon \in [1.0, 5.0]$ as a practically useful operating range, achieving evidence-recovery accuracy of 73–86% while providing formal privacy guarantees. High-sensitivity domains such as healthcare and banking should operate at lower epsilon values, accepting a modest accuracy trade-off to satisfy strict regulatory obligations. Significant open research challenges remain, including the absence of standardised forensic device interfaces, the need for Byzantine-robust evidence aggregation in federated forensics pipelines, the forensic-ready-by-design paradigm, and the adversarial robustness of AI-based forensic tools. Addressing these challenges requires interdisciplinary collaboration spanning digital forensic science, privacy engineering, distributed systems, and law.

5.2 Limitations

- Our analysis is based on a systematic literature review; hence, there is no experimental data to base our analysis on. Hence, the reported performance values are based on various experimental conditions and do not lend themselves to statistical combination or aggregation.
- Domain-level differential privacy trade-offs have been considered, but device/protocol-specific ones within the different domains have not been discussed.
- In this review, grey literature, theses, and patents were excluded; therefore, it is possible that not all current or emerging practical applications are covered if they have not yet appeared in peer-reviewed journals.
- Six methods were included in the comparison of performance; composite or ensemble forensics were not included.
- Due to the fast-paced nature of IoT standards and security, it is possible that some of the performance figures may soon become outdated. The searches were confined to papers published up to March 2025.

5.2 Future Scope

- Work must be undertaken to create generic forensic acquisition interfaces for IoT, similar to JTAG in traditional computation. Such interfaces would provide repeatable and tool-independent evidence acquisition for diverse IoT device families.
- The adoption and rigorous evaluation of Byzantine-robust aggregation techniques such as Krum and Trimmed Mean to federated IoT forensic pipelines operating on non-IID evidence streams is crucial.
- Proactive forensic readiness frameworks - where cryptographically secure and lightweight logging of evidence is integrated into IoT devices at design time- can effectively tackle the challenge of evidence volatility.
- The adversarial robustness of AI/ML-based forensic detection models against traffic perturbation attacks has to be empirically assessed using tools and techniques from adversarial machine learning.

- Future surveys need to incorporate and cover hybrid approaches to forensics, such as those combining FaaS, blockchain and differential privacy and evaluate them on new IoT benchmarks in smart city and industrial IoT applications.

6. CONFLICT OF INTEREST

The authors declare no conflicts of interest regarding the publication of this research.

REFERENCES

[1] Garg, P., Dixit, A., & Sethi, P. (2022). Ml-fresh: novel routing protocol in opportunistic networks using machine learning. *Computer Systems Science & Engineering, Forthcoming*. Tech Science Press.

[2] Yadav, P. S., Khan, S., Singh, Y. V., Garg, P., & Singh, R. S. (2022). A Lightweight Deep Learning-Based Approach for Jazz Music Generation in MIDI Format. *Computational Intelligence and Neuroscience*, *2022*.

[3] Soni, E., Nagpal, A., Garg, P., & Pinheiro, P. R. (2022). Assessment of Compressed and Decompressed ECG Databases for Telecardiology Applying a Convolution Neural Network. *Electronics*, *11*(17), 2708.

[4] Pustokhina, I. V., Pustokhin, D. A., Lydia, E. L., Garg, P., Kadian, A., & Shankar, K. (2021). Hyperparameter search-based convolutional neural network with Bi-LSTM for an intrusion detection system in a multimedia big data environment. *Multimedia Tools and Applications*, 1-18.

[5] Khanna, A., Rani, P., Garg, P., Singh, P. K., & Khamparia, A. (2021). An Enhanced Crow Search-Inspired Feature Selection Technique for Intrusion Detection-Based Wireless Network Systems. *Wireless Personal Communications*, 1-18.

[6] Garg, P., Dixit, A., Sethi, P., & Pinheiro, P. R. (2020). Impact of node density on the QoS parameters of routing protocols in opportunistic networks for smart spaces. *Mobile Information Systems*, *2020*.

[7] Upadhyay, D., Garg, P., Aldossary, S. M., Shafi, J., & Kumar, S. (2023). A Linear Quadratic Regression-Based Synchronised Health Monitoring System (SHMS) for IoT Applications. Electronics, 12(2), 309.

[8] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). CNN-BI-LSTM-CYP: A deep learning approach for sugarcane yield prediction: Sustainable *Energy Technologies and Assessments*, *57*, 103263.

[9] Saini, P., Nagpal, B., Garg, P., & Kumar, S. (2023). Evaluation of Remote Sensing and Meteorological Parameters for Yield Prediction of Sugarcane (Saccharum officinarum L.) Crop. Brazilian Archives of Biology and Technology, 66, e23220781.

[10] Beniwal, S., Saini, U., Garg, P., & Joon, R. K. (2021). Improving performance during camera surveillance by integrating edge detection into an IoT system. *International Journal of E-Health and Medical Communications (IJEHMC)*, *12*(5), 84-96.

[11] Garg, P., Dixit, A., & Sethi, P. (2019). Wireless sensor networks: an insight review. *International Journal of Advanced Science and Technology*, *28*(15), 612-627.

[12] Sharma, N., & Garg, P. (2022). Ant colony-based optimisation model for QoS-Based task scheduling in cloud computing environment—measurement*: Sensors*, 100531.

[13] Kumar, P., Kumar, R., & Garg, P. (2020). Hybrid Crowd Cloud Routing Protocol For Wireless Sensor Networks. *International Journal of Advanced Science and Technology*, *29*, 766-775.

[14] Raj, G., Verma, A., Dalal, P., Shukla, A. K., & Garg, P. (2023). Performance Comparison of Several LPWAN Technologies for Energy-Constrained IoT Network. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(1s), 150-158.

[15] Garg, P., Sharma, N., & Shukla, B. (2023). Predicting the Risk of Cardiovascular Diseases using Machine Learning Techniques. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(2s), 165-173.

[16] Patil, S. C., Mane, D. A., Singh, M., Garg, P., Desai, A. B., & Rawat, D. (2024). Parkinson's Disease Progression Prediction Using Longitudinal Imaging Data and Grey Wolf Optimiser-Based Feature Selection. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), 441-451.

[17] Gudur, A., Pati, P., Garg, P., & Sharma, N. (2024). Radiomics Feature Selection for Lung Cancer Subtyping and Prognosis Prediction: A Comparative Study of Ant Colony Optimisation and Simulated Annealing. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3s), 553-565.

[18] Khan, A. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *J. Electrical Systems*, *20*(6s), 1051-1058.

[19] Sharma, K. K., Verma, P. K., & Garg, P. (2024). IoT-Enabled Energy Management Systems For Sustainable Energy Storage: Design, Optimisation, And Future Directions. *Frontiers in Health Informatics*, *13*(8).

[20] Gupta, S., Yadav, N., Singh, K., & Garg, P. (2025). APPLICATIONS OF SIMULATIONS AND QUEUING THEORY IN A SUPERMARKET *Reliability: Theory & Applications*, *20*(1 (82)), 135-140.

[21] Beniwal, S., Garg, P., Rajpal, R., Sharma, N., & Mittal, H. K. (2025). Fusion of Opportunistic Networks with Machine Learning: Present and Future. *Metallurgical and Materials Engineering*, *31*(1), 311-324.

[22] Garg, P. (2025). Explainable AI & Model Interpretability in Healthcare: Challenges & Future Directions. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, *46*(1), 104-133.

[23] Rani, P. (2025). From Data to Diagnosis: Unleashing AI and 6G in Modern Medicine. *EKSPLORIUM-BULETIN PUSAT TEKNOLOGI BAHAN GALIAN NUKLIR*, *46*(1), 69-103.

[24] Dixit, A., Garg, P., Sethi, P., & Singh, Y. (2020, April). TVCCCS: Television Viewer's Channel Cost Calculation System on Per-Second Usage. In *IOP Conference Series: Materials Science and Engineering* (Vol. 804, No. 1, p. 012046). IOP Publishing.

[25] Sethi, P., Garg, P., Dixit, A., & Singh, Y. (2020, April). Smart number cruncher–a voice-based calculator. In *IOP Conference Series: Materials Science and Engineering* (Vol. 804, No. 1, p. 012041). IOP Publishing.

[26] S. Rai, V. Choubey, Suryansh and P. Garg, "A Systematic Review of Encryption and Keylogging for Computer System Security," *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, 2022, pp. 157-163, doi: 10.1109/CCiCT56684.2022.00039.

[27] L. Saraswat, L. Mohanty, P. Garg and S. Lamba, "Plant Disease Identification Using Plant Images," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 79-82, doi: 10.1109/CCiCT56684.2022.00026.

[28] L. Mohanty, L. Saraswat, P. Garg and S. Lamba, "Recommender Systems in E-Commerce," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 114-119, doi: 10.1109/CCiCT56684.2022.00032.

[29] C. Maggo and P. Garg, "From linguistic features to their extractions: Understanding the semantics of a concept," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 427-431, doi: 10.1109/CCiCT56684.2022.00082.

[30] N. Puri, P. Saggar, A. Kaur and P. Garg, "Application of ensemble Machine Learning models for phishing detection on web networks," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 296-303, doi: 10.1109/CCiCT56684.2022.00062.

[31] R. Sharma, S. Gupta and P. Garg, "Model for Predicting Cardiac Health using Deep Learning Classifier," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 25-30, doi: 10.1109/CCiCT56684.2022.00017.

[32] Varshney, S. Lamba and P. Garg, "A Comprehensive Survey on Event Analysis Using Deep Learning," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), 2022, pp. 146-150, doi: 10.1109/CCiCT56684.2022.00037.

[33] Dixit, A., Sethi, P., Garg, P., & Pruthi, J. (2022, December). Speech Difficulties and Clarification: A Systematic Review. In *2022, the 11th International Conference on System Modelling & Advancement in Research Trends (SMART)* (pp. 52-56). IEEE.

[34] Garg, P., Dixit, A., Sethi, P., & Pruthi, J. (2023, December). Strengthening Smart City with Opportunistic Networks: An Insight. In the *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 700-707). IEEE.

[35] Rana, S., Chaudhary, R., Gupta, M., & Garg, P. (2023, December). Exploring Different Techniques for Emotion Detection Through Face Recognition. In *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 779-786). IEEE.

[36] Mittal, K., Srivastava, K., Gupta, M., & Garg, P. (2023, December). Exploration of Different Techniques on Heart Disease Prediction. In *2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech)* (pp. 758-764). IEEE.

[37] Gautam, V. K., Gupta, S., & Garg, P. (2024, March). Automatic Irrigation System using IoT. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 100-103). IEEE.

[38] Ramasamy, L. K., Khan, F., Joghee, S., Dempere, J., & Garg, P. (2024, March). Forecast of Students' Mental Health Combining an Artificial Intelligence Technique and Fuzzy Inference System. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 85-90). IEEE.

[39] Rajput, R., Sukumar, V., Patnaik, P., Garg, P., & Ranjan, M. (2024, March). The Cognitive Analysis for an Approach to Neuroscience. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 524-528). IEEE.

[40] Dixit, A., Sethi, P., Garg, P., Pruthi, J., & Chauhan, R. (2024, July). CNN-based lip-reading system for visual input: A review. In *AIP Conference Proceedings* (Vol. 3121, No. 1). AIP Publishing.

[41] Bose, D., Arora, B., Srivastava, A. K., & Garg, P. (2024, May). A Computer Vision-Based Framework for Posture Analysis and Performance Prediction in Athletes. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 942-947). IEEE.

[42] Singh, M., Garg, P., Srivastava, S., & Saggu, A. K. (2024, April). Revolutionising Arrhythmia Classification: Unleashing the Power of Machine Learning and Data Amplification for Precision Healthcare. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 516-522). IEEE.

[43] Kumar, R., Das, R., Garg, P., & Pandita, N. (2024, April). Duplicate Node Detection Method for Wireless Sensors. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 512-515). IEEE.

[44] Bhardwaj, H., Das, R., Garg, P., & Kumar, R. (2024, April). Handwritten Text Recognition Using Deep Learning. In *2024 Sixth International Conference on Computational Intelligence and Communication Technologies (CCICT)* (pp. 506-511). IEEE.

[45] Gill, A., Jain, D., Sharma, J., Kumar, A., & Garg, P. (2024, May). Deep learning approach for facial identification for online transactions. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 715-722). IEEE.

[46] Mittal, H. K., Dalal, P., Garg, P., & Joon, R. (2024, May). Forecasting Pollution Trends: Comparing Linear, Logistic Regression, and Neural Networks. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 411-419). IEEE.

[47] Malik, T., Nandal, V., & Garg, P. (2024, May). Deep Learning-Based Classification of Diabetic Retinopathy: Leveraging the Power of VGG-19. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 645-651). IEEE.

[48] Srivastava, A. K., Verma, I., & Garg, P. (2024, May). Improvements in Recommendation Systems Using Graph Neural Networks. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 668-672). IEEE.

[49] Aggarwal, A., Jain, D., Gupta, A., & Garg, P. (2024, May). Analysis and Prediction of Customer Churn and Retention Rates in the Telecom Industry Using Logistic Regression. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 723-727). IEEE.

[50] Mittal, H. K., Arsalan, M., & Garg, P. (2024, May). A Novel Deep Learning Model for Effective Story Point Estimation in Agile Software Development. In *2024 International Conference on Emerging Innovations and Advanced Computing (INNOCOMP)* (pp. 404-410). IEEE.

[51] Shukla, S. M., Magoo, C., & Garg, P. (2024, November). Comparing Fine-Tuned LMs for Detecting LLM-Generated Text. In *2024, the 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)* (pp. 1-8). IEEE.

[52] Kumar, B., IQBAL, M., Parmer, R., Garg, P., Rani, S., & Agrawal, A. (2025, March). The Role of AI in Optimising Healthcare Appointment Scheduling. In *2025, the 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 881-887). IEEE.

[53] Kumar, B., Garg, V., Ahmed, K., Garg, P., Choudhary, S., & Baniya, P. (2025, March). Enhancing Healthcare with Blockchain: Innovations in Data Privacy, Security, and Interoperability. In *2025, the 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 932-938). IEEE.

[54] Raj, V., Prakash, B. K., Kumar, A., & Garg, P. (2024, December). Optimise the Time a Mercedes-Benz Spends on the Test Bench Using Stacking Ensemble Learning. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 445-450). IEEE.

[55] Kaushik, N., Kumar, H., Raj, V., & Garg, P. (2024, December). Proactive Fault Prediction in Microservices Applications Using Trace Logs and Monitoring Metrics. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 410-415). IEEE.

[56] Kumar, A. A., Sri, C. V., Bohara, K. S. K., Setia, S., & Garg, P. (2024, December). Capnivesh: Financing Platform for Startups. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 261-265). IEEE.

[57] Bhandari, P., Setia, S., Kumar, K., & Garg, P. (2024, December). Optimising Cross-Platform Development with CI/CD and Containerization: A Review. In *2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS)* (pp. 175-180). IEEE.

[58] Chaudhary, A., & Garg, P. (2014). Detecting and diagnosing a disease using a patient monitoring system. *International Journal of Mechanical Engineering And Information Technology*, *2*(6), 493-499.

[59] Malik, K., Raheja, N., & Garg, P. (2011). Enhanced FP-growth algorithm. *International Journal of Computational Engineering and Management*, *12*, 54-56.

[60] Garg, P., Dixit, A., & Sethi, P. (2021, May). Link Prediction Techniques for Opportunistic Networks using Machine Learning, in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.

[61] Garg, P., Dixit, A., & Sethi, P. (2021, April). Opportunistic networks: Protocols, applications & simulation trends. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*.

[62] Garg, P., Dixit, A., & Sethi, P. (2021). Performance comparison of the fresh and spray-and-wait protocols using a single simulator. *IT in Industry*, *9*(2).

[63] Malik, M., Singh, Y., Garg, P., & Gupta, S. (2020). Deep Learning in the Healthcare System. *International Journal of Grid and Distributed Computing*, *13*(2), 469-468.

[64] Gupta, M., Garg, P., Gupta, S., & Joon, R. (2020). A Novel Approach for Malicious Node Detection in Cluster-Head Gateway Switching Routing in Mobile Ad Hoc Networks. *International Journal of Future Generation Communication and Networking*, *13*(4), 99-111.

[65] Gupta, A., Garg, P., & Sonal, Y. S. (2020). Edge Detection-Based 3D Biometric System for Security of Web-Based Payment and Task Management Application. *International Journal of Grid and Distributed Computing*, *13*(1), 2064-2076.

[66] Garg, P., & Raman, P. K. (2011). Broadcasting Protocol & Routing Characteristics in Wireless Ad Hoc Networks. *Int. J. Comput. Emg. Manag*, *12*(1), 36-40.

[67] Garg, P., Arora, N., & Malik, T. (2011). Capacity Improvement of Wi-MAX in the presence of Different Codes WI-MAX: Speed & Scope of the future. *IJCEM*, *12*.

[68] Garg, P., Saroha, K., & Lochab, R. (2011). Review of wireless sensor networks: architecture and applications. IJCSMS International Journal of Computer Science & Management Studies, 11(01), 2231-5268.

[69] Yadav, S., &Garg, P. Development of a New Secure Algorithm for Encryption and Decryption of Images.

[70] Dixit, A., Sethi, P., & Garg, P. (2022). Rakshak: A Child Identification Software for Recognising Missing Children Using Machine Learning-Based Speech Clarification. International Journal of Knowledge-Based Organisations (IJKBO), 12(3), 1-15.

[71] Shukla, N., Garg, P., & Singh, M. (2022). MANET Proactive and Reactive Routing Protocols: A Comparison Study. International Journal of Knowledge-Based Organisations (IJKBO), 12(3), 1-14.

[72] Arya, A., Garg, P., Vellanki, S., Latha, M., Khan, M. A., & Chhbra, G. (2024). Optimisation Methods Based on Soft Computing for Improving Power System Stability. *Journal of Electrical Systems*, *20*(6s), 1051-1058.

[73] Garg, P. (2025). Cloud security posture management: Tools and techniques. Technix International Journal for Engineering Research, 12(3).

[74] Tyagi, P., Sharma, S., Srivastava, A., Rajput, N. K., Garg, P., & Kumari, M. (2025). AI in Healthcare: Transforming Medicine with Intelligence. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p4

[75] Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges, and Future Prospects. *Applications, Challenges, and Future Prospects (May 17, 2025)*.

[76] Garg, P., Saraswat, P., & Siddiqui, Z. (2025). AI & the Indian Stock Market: A Review of Applications in Investment Decision. https://doi.org/10.63169/GCARED2025.p10

[77] Garg, P., Sharma, S., Mittal, S., Tevatia, R., Tyagi, V. K., & Kapoor, S. (2025). Unlocking Workforce Potential: AI-Powered Predictive Models for Employee Performance Evaluation. https://doi.org/10.63169/GCARED2025.p21

[78] Shrivas, N., Kalia, A., Roy, R., Sharma, S., Garg, P., & Agarwal, G. (2025). OSINT: A Double-edged Sword. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p22

[79] Garg, P., Aditi, A., & Roy, B. (2025). A System of Computer Network: Based On Artificial Intelligence. https://doi.org/10.63169/GCARED2025.p24

[80] Parmar, R., Kapoor, S., Saifi, S., & Garg, P. (2025). Case Study on Intelligent Factory Systems for Improving Productivity and Capability in Industry 4.0 with Generative AI. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p28

[81] Singh, R., Sharma, R., Kumar, R., Nafis, A., Siddiqui, M. A. M., & Garg, P. (2025). Detection of Unauthorised Construction using Machine Learning: A Review. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p30

[82] Garg, P., Kapoor, S., Singh, V., Sharma, S., & Ankita, A. (2025). A Bridge between Blockchain and Decentralised Applications, Web3 and Non-Web3 Crypto Wallets. https://doi.org/10.63169/GCARED2025.p35

[83] Verma, M., Sharma, S., Garg, P., & Singh, A. (2025). The Hidden Dangers of Prototype Pollution: A Comprehensive Detection Framework. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p36

[84] Sharma, A., Sharma, S., Garg, P., & Bhardwaj, P. (2025). LockTalk: A Basic Secure Chat Application. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India.

[85] Arora, K., Bawane, R., Gupta, C., Ahmed, K., & Garg, P. (2025). Detection and Prevention of Cyber Attacks and Threats using AI. In the *First Global Conference on AI Research and Emerging Developments (G-CARED 2025)*, New Delhi, India. https://doi.org/10.63169/GCARED2025.p38

[86] Garg, P., Dhruv, D., Rahman, A. A., Rai, A., Siddiqui, M., & Yadav, D. (2025). Easeviewer: An Esports Production Tool. https://doi.org/10.63169/GCARED2025.p46

[87] Garg, P., Lakshita, L., Mehwish, M., Nazia, N., & Ahmed, K. (2025). Emerging Trend in Computational Technology: Innovations, Applications, and Challenges. *Applications and Challenges (May 17, 2025)*. https://doi.org/10.63169/GCARED2025.p51

[88] Chauhan, S., Singh, M., & Garg, P. (2021). Rapid Forecasting of Pandemic Outbreak Using Machine Learning. *Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies*, 59-73.

[89] Gupta, S., & Garg, P. (2021). An insight review on multimedia forensics technology. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 27.

[90] Shrivastava, P., Agarwal, P., Sharma, K., & Garg, P. (2021). Data leakage detection in Wi-Fi networks. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 215.

[91] Meenakshi, P. G., & Shrivastava, P. (2021). Machine learning for mobile malware analysis. *Cyber Crime and Forensic Computing: Modern Principles, Practices, and Algorithms*, *11*, 151.

[92] Nanwal, J., Garg, P., Sethi, P., & Dixit, A. (2021). Green IoT and Big Data: Succeeding towards Building Smart Cities. In *Green Internet of Things for Smart Cities* (pp. 83-98). CRC Press.

[93] Gupta, M., Garg, P., & Agarwal, P. (2021). Ant Colony Optimisation Technique in Soft Computational Data Research for NP-Hard Problems. In *Artificial Intelligence for a Sustainable Industry 4.0* (pp. 197-211). Springer, Cham.

[94] Magoo, C., & Garg, P. (2021). Machine Learning Adversarial Attacks: A Survey Beyond. *Machine Learning Techniques and Analytics for Cloud Security*, 271-291.

[95] Garg, P., Srivastava, A. K., Anas, A., Gupta, B., & Mishra, C. (2023). Pneumonia Detection Through X-Ray Images Using Convolution Neural Network. In *Advancements in Bio-Medical Image Processing and Authentication in Telemedicine* (pp. 201-218). IGI Global.

[96] Gupta, S., & Garg, P. (2023). 14 Code-based post-quantum cryptographic technique: digital signature. *Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity*, 193.

[97] Prakash, A., Avasthi, S., Kumari, P., & Rawat, M. (2023). PuneetGarg 18 Modern healthcare system: unveiling the possibility of quantum computing in medical and biomedical zones. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 249.

[98] Gupta, S., & Garg, P. (2024). Mobile Edge Computing for Decentralised Systems. *Decentralised Systems and Distributed Computing*, 75-88.

[99] Gupta, M., Garg, P., & Malik, C. (2024). Ensemble learning-based analysis of perinatal disorders in women. In Artificial Intelligence and Machine Learning for Women's Health Issues (pp. 91-105). Academic Press.

[100] Malik, M., Garg, P., & Malik, C. (2024). Artificial intelligence-based prediction of health risks among women during menopause. *Artificial Intelligence and Machine Learning for Women's Health Issues*, 137-150.

[101] Garg, P. (2024). Prediction of female pregnancy complications using artificial intelligence. In *Artificial Intelligence and Machine Learning for Women's Health Issues* (pp. 17-35). Academic Press.

[102] Pokhrel, L., Arsalan, M., Rani, P., Garg, P., & Pinheiro, P. R. (2026). AI-Powered Healthcare Solutions: Bridging the Medical Gap in Underserved Communities Worldwide. In *Applied AI and Computational Intelligence in Diagnostics and Decision-Making* (pp. 57-86). IGI Global Scientific Publishing.

[103] Kapoor, S., Parmar, R., Sharma, N., Garg, P., & Singh, N. J. (2026). AI and Computational Intelligence in Healthcare: An Introductory Guide. In *Applied AI and Computational Intelligence in Diagnostics and Decision-Making* (pp. 1-26). IGI Global Scientific Publishing.

[104] Pokhrel, L., Kumar, A., Garg, P., Anand, N., & Singh, N. (2026). AI and IoT in Global Health: Ethical Lessons From Pandemic Response. In *Development and Management of Eco-Conscious IoT Medical Devices* (pp. 367-394). IGI Global Scientific Publishing.

[105] Parmar, R., Singh, A., Garg, P., Sharma, T., & Pinheiro, P. R. (2026). Blockchain for Ethical Supply Chains: Transparency in Medical IoT Manufacturing. In *Development and Management of Eco-Conscious IoT Medical Devices* (pp. 337-366). IGI Global Scientific Publishing.

[106] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2024). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 1). https://doi.org/10.2174/9789815313031124030l

[107] Gupta, S., Chaudhary, G., & Garg, P. (2013). Modified AODV Routing Protocol through Cache Memory for Finding New Routing Paths in MANETs—International *Journal of Computer Science & Management Studies*, *13*(3).

[108] Gupta, A., & Garg, P. (2021). Emerging Techniques for Handling Pandemic Challenges. *Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies*, 189-209.

[109] Chaudhary, A. P., Mishra, A., Kumar, D., & Garg, P. (2023, April). Human Emotion Recognition using Deep Learning. In the *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)* (pp. 191-197). IEEE.

[110] Nagpal, S., Garg, P., Gaba, S., & Aggarwal, A. (2023). 13 An improved genetic quantum cryptography model for network communication. *Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity*, 177.

[111] Yadav, M., Swami, V., Kumar, N., & Garg, P. (2025). Comparative study of Repairable Juice Plants using RPGT. *Reliability: Theory & Applications*, *20*(2 (84)), 776-783.

[112] Gupta, A., Garg, P., & Yadav, P. (2025). Role of Generative AI Towards Education and Learning: Present & Future. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S6 (2025): Posted 15 Sept), 1059-1076.

[113] Dalal, P., Beniwal, G., Sharma, V., Garg, P., & Ahmed, K. (2025). Predicting Student Motivation and Engagement through Machine Learning Models. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 393-411.

[114] Gupta, A., Mund, A., Roy, S., Garg, P., & Yadav, D. K. (2025). Trust in AI Systems: A Social-psychological Investigation of Human–AI Collaboration. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 428-446.

[115] Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2025). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analogue Applications: Bhardwaj, Das, Garg, and Yadav. *Journal of Electronic Materials*, 1-12.

[116] Dalal, P., Sharma, B., Sharma, T., Garg, P., & Ahmed, K. (2025). Explainable AI for Understanding Human Decision-Making Patterns. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S7 (2025): Posted 10 October), 412-427.

[117] Sharma, K. K., Verma, P. K., Garg, P., & Shrotriya, V. K. (2025, October). Predicting costs and benefits of IoT-based energy management for optimising sustainable energy storage in rural areas. In *AIP Conference Proceedings* (Vol. 3343, No. 1, p. 040017). AIP Publishing LLC.

[118] Ahmed, K., Baranwal, A., Sharma, N., Garg, P., & Singh, N. (2026). The Role of Federated Learning in AI-Powered Integrated Healthcare Solutions. In *Enabling Collaborative Health Intelligence With Federated Learning* (pp. 421-448). IGI Global Scientific Publishing.

[119] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (2025). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 2). Bentham Science Publishers. https://doi.org/10.2174/9789815322241250301

[120] Garg, P., Pranav, S., & Prerna, A. (2021). Green internet of things (G-IoT): A solution for sustainable technological development. In *Green Internet of Things for Smart Cities* (pp. 23-46). CRC Press.

[121] Malik, A., Nandal, D., Gupta, V., Garg, P., & Nandal, V. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[122] Gupta, S., Garg, P., Agarwal, J., Thakur, H. K., & Yadav, S. P. (Eds.). (2025). Federated learning-based intelligent systems to handle issues and challenges in IoVs (Part 2).

[123] Garg, P., Bhatt, M., Parmar, R., & Arsalan, M. (2025). Generative AI: Evolution, Applications, Challenges, and Future Prospects. *Applications, Challenges, and Future Prospects (May 17, 2025)*.

[124] Kumar, N., Kumar, Y., Khurana, D., Kumar, S., & Garg, P. (2025, November). A Hybrid Ensemble Learning Framework for Interpretable Student Performance Prediction Using Academic and Extracurricular Factors. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 666-672). IEEE.

[125] Khurana, D., Kumar, Y., Kumar, N., Kumar, S., & Garg, P. (2025, November). Transformer-Based Movie Recommendation System with Autoencoder-Enhanced Feature Compression. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 685-690). IEEE.

[126] Garg, P. (2025, November). Comparative Analysis of Various Neural Networks for Galaxy Classification. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 697-701). IEEE.

[127] Saggu, A. K., Babbar, N., & Garg, P. (2025, November). Health-Guard AI: Integrated Health Report Management and Analysis. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 614-623). IEEE.

[128] Kumar, S., Kumar, Y., Kumar, N., Khurana, D., & Garg, P. (2025, November). Hybrid FCM-DNN Model for Uncertainty-Aware Air Quality Classification Using Multi-Pollutant Data. In *2025 International Conference on Innovations and Emerging Technologies in AI & Communication Systems (IETACS)* (pp. 679-684). IEEE.

[129] Babbar, N., Singh, H. V., Bendale, S., & Garg, P. (2025, November). Stock Market Price Prediction Using Big Data Analysis: A Performance Evaluation Study. In *2025, the 3rd International Conference on Computational Intelligence and Network Systems (CINS)* (pp. 1-6). IEEE.

[130] Singh, A. K., Kori, G., Garg, P., & Srivastava, G. (2025, November). Bank Churn Prediction Using Machine Learning. In *2025, IEEE 7th International Conference on Computing, Communication and Automation (ICCCA)* (pp. 1-6). IEEE.

[131] Bhardwaj, A., Das, A., Garg, P., & Yadav, S. (2026). Material-Driven Performance Analysis of a Vertical Nanowire Tunnel FET for Analogue Applications. *Journal of Electronic Materials*, *55*(1), 1099-1110.

[132] Srivastava, A. K., Shankdhar, D., Ror, R., & Garg, P. (2026). Harnessing YOLOv5 for real-time object detection: A cloud-based approach. In *Recent Advances in Computational Methods in Science and Technology* (pp. 441-450). CRC Press.

[133] Srivastava, A. K., Shukla, A., Gupta, H., Saxena, K., & Garg, P. (2026). Towards an intelligent attendance management system with face recognition using the LBPH algorithm. In *Recent Advances in Computational Methods in Science and Technology* (pp. 8-15). CRC Press.

[134] Srivastava, A. K., Garg, P., & Pandey, H. (2026). Vedcure: Towards intelligent ayurvedic drug recommendation and disease prediction. In *Recent Advances in Computational Methods in Science and Technology* (pp. 16-23). CRC Press.

[135] Upadhyay, D., Garg, P., & Babbar, N. (2026). A blockchain- and IoT-based smart contract framework for efficient and secure product lifecycle management. *Discover Internet of Things*.

[136] Singh, A., Parmar, R., Bhardwaj, P., Sharma, V., & Garg, P. (2026). Fusion of Aerial Networks with Advanced Computing Paradigms. *Edge Computing and Aerial Platforms*, 355-367.

[137] Kumari, M., Baranwal, A., Sonal, & Garg, P. (2026). Application of Aerial Edge Computing in Disaster Management. *Edge Computing and Aerial Platforms*, 103-122.

[138] Aditi, Saraswat, P., Sharma, V., & Garg, P. (2026). Advances in Aerial Platforms and Edge Computing. *Edge Computing and Aerial Platforms*, 123-143.

[139] Garg, P., Arora, K., Bawane, R., Gupta, C., & Ahmed, K. (2025). Detection and Prevention of Cyber Attacks and Threats using AI.

[140] Ahmed, K., Ahmed, A., Khan, J., Garg, P., Seth, S., & Mallik, S. (2025). Principal Component Analysis-Based Clustering of Insecticides and Molecular Docking of Pyrethroid Insecticides.

[141] Kumar, B., Kumar, A., Nanwal, J., Garg, P., & Patnaik, P. (2025, November). Ensemble of YOLOv5 and Segment Anything Model for Brain Tumour Detection. In *2025, the 2nd International Conference on Advanced Computing and Emerging Technologies (ACET)* (pp. 1-5). IEEE.

[142] Arsalan, M., Anas, M., & Garg, P. (2025). Transparent AI for Drug Discovery and Development. *Available at SSRN 5844242*.

[143] Singh, A., Bhardwaj, P., Garg, P., & Singh, N. (2026). Introduction to explainable artificial intelligence in healthcare. In *Explainable AI in Clinical Practice* (pp. 23-44). Academic Press.

[144] Kapoor, S., Singh, A., Garg, P., & Ramasamy, L. K. (2026). Explainable artificial intelligence in a diagnostic support system. In *Explainable AI in Clinical Practice* (pp. 131-145). Academic Press.

[145] Ahmed, K., Anas, M., & Garg, P. (2026). Case studies on unlocking the potential of Industry 4.0 for sustainable manufacturing through generative AI-driven innovations. *Available at SSRN 6356958*.

[146] Garg, P., & Oruganti, S. K. (2026, March). AI Assisted Routing Optimisation in Opportunistic IoT Networks using Machine Learning: A Comprehensive Review on Protocols & Simulators. In *Sustainable Global Societies Initiative* (Vol. 1, No. 4). Vibrasphere Technologies.

[147] Arsalan, M., Pokhrel, L., & Garg, P. (2026). Architecture, Components, and tools in Integrated AI-Augmented Intelligence: A design perspective. *Components and tools in Integrated AI-Augmented Intelligence: A design perspective (March 19, 2026)*.

[148] Singh, H., Ahmed, K., & Garg, P. (2026). Human Versus Machine Customer Behaviour and Functional Differences. *Available at SSRN 6441098*.

[149] Saraswat, P., & Garg, P. (2026). Soft Computing In AI Agents.

[150] Saraswat, P., & Garg, P. (2026). Water Quality Prediction Using IOT Sensors and Deep Networks.