COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 6, Issue 1, Jan-Jun 2026, pp. 1-28
DOI: 10.17492/computology.v6i1.2601
https://www.journalpressindia.com/cjacsit

Integrating Internet of Thing (IoT) Technologies into Forensic Science: Advancements, Applications and Challenges in Crime Scene Investigation

Ria Ghosh and Sreenath Sreekantan***

ABSTRACT

The actual-time introduction of IoT technologies in the modern life has certainly changed the sphere of forensic science, and especially in the realm of crime scene investigation. This manuscript will provide an in-depth account of the development, existing uses and the limitations that come with the use of IoT data in forensics. As seen in the discussion, the real-time monitoring, geolocation, and automatics of a networked device can help to protect evidence, profile suspected criminals, and recreate a crime with more accuracy. Legal and ethical aspects including the privacy, use of IoT based data in the courts as evidence and technology challenges of encryption, protection of data and interoperability, the Future of AI, Blockchain, and Edge Computing in IoT-Based Forensic Analysis are also included in this study. Incorporated within the framework of modern case studies and innovative application, the article explains the revolutionary nature of the use of the IoTs in forensics and its evolution and the need to adopt solid, standardised and responsible practices. The conclusions are expected to enlighten the practitioners and policymakers on the revolution of forensic science in the 21st century which will ultimately offer increased efficacy, usefulness, and jurisprudence in the crime scene investigations.

Keywords: *Internet of Things (IoT); Digital forensics; Smart devices; Geolocation tracking; Artificial intelligence; Crime scene investigation; Digital evidence; Legal admissibility.*

1.0 Introduction

The Internet of Things (IoT) revolutionized modern forensic science, fundamentally changing the processes of crime scene investigations and becoming ubiquitous in nature.

**Corresponding author; Research Scholar, Digital Forensics and Cybersecurity, Indian Institute of Technology Patna, Bihar, India (E-mail: ria2024ghosh@gmail.com)*
***Emergency Medicine Doctor, Medicine, National Health Service (NHS), England, United Kingdom (E-mail: s.sreekantan@nhs.net)*

IoT is not limited to home automation, wearable gadgets, connected cars, or sophisticated surveillance systems; it is, in fact, a system of interconnected physical objects that utilize sensors, software, and connectivity to gather, transmit, and exchange data over the internet. The requirement of IoT in policing goes back to the era of digital video cameras and sensor-equipped security regulations. With the devices getting more active and (invariably) connected, millions of these now-ubiquitous environments give up huge streams of real-time data which could just contain the clue to not only the factual evidence of a crime. Nowadays, when practically all electronic appliances turned into the IoT, the paradigm of presence and consistency of digital evidence ceased to be among restricted access of a person using a range of locations, including houses, offices, and fields (Abomhara & Koien, 2015). Most of the crime investigators are able to access the information of the home security alarms, the fitness watches, cars telematics systems, or other devices that can store or transmit the timestamps, movement records, locations and even biometric information. These are computer records, which are usually linked to particular activities or incidents and have been instrumental in re-creating the crime scenes, authenticating the witnesses and suspect trails. With the application of innovative analytical tools, including AI and machine learning, forensic professionals are now able to process large volumes of data much more quickly, and using the resulting trends, make viable recommendations.

Although IoT is not going away, and it can greatly assist in forensic work, it has its share of challenges to its introduction. Besides, the issue of data privacy and security have been discussed on the floor since the dawn of time, as well as has the admissibility of evidence produced by the IoT devices in the court. The current encryption of device data, absence of standardisation and the efficacy of manufacturer support of extracting and validating the evidence may hinder the extraction of evidence. Besides, the threats of physical evidence manipulation, which may get even bigger due to the change in jurisdictions of the case, imply an urgent necessity to enforce the regulations and introduce the forensic practices that can be easily reproduced. Ethical concerns are also posed by surveillance and bulk data collection and these should be highly considered in balance to the right of the citizens and open practices of evidence management (Ahmed *et al.*, 2024).

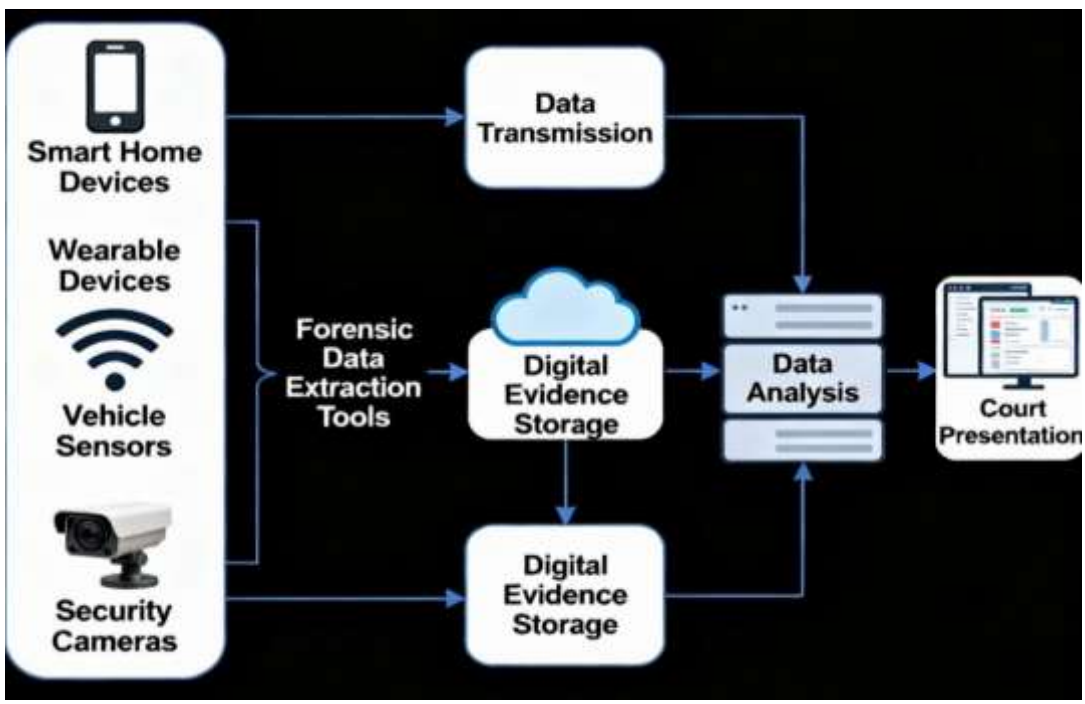
The chapter discusses the key role that IoT plays in the crime scene investigation, including its existing applications and the major challenges that should be considered. It reveals the new face of forensic investigation in a high-tech world and provides a backdrop against which one can discuss the new efforts in the future, such as edge computing and blockchain authentication, which can be utilized to enhance the security and integrity of IoT evidence. Internet of things is potential to cause revolution in crime fighting as the technology will not only introduce technology in criminal justice, it will introduce change

on how crime scenes are investigated and it will be more focused and quicker and even solvable in the digital era as well as being data-driven.

2.0 Understanding IoT in Crime Scene Investigation

The Internet of Things is a major paradigm shift in forensic investigations, and the new opportunities presented by the Internet of Things can be used to collect, analyse, and reconstruct evidence in a crime scene. Essentially, the Internet of Things refers to a wide range of internet-connected physical devices equipped with sensors, software, and the capability to send and store data about real-world events. With wearables, smart homes, smart cars, and drones, the proliferation of these devices has transformed the modern crime scene into a coroner's nightmare of ill-got digital footprints awaiting forensic analysis. In Figure 1, the schematic diagram illustrates how IoT devices are used and integrated in crime scene investigation (CSI).

Figure 1: Schematic Diagram Showing the Integration and Workflow of IoT Devices in Crime Scene Investigation

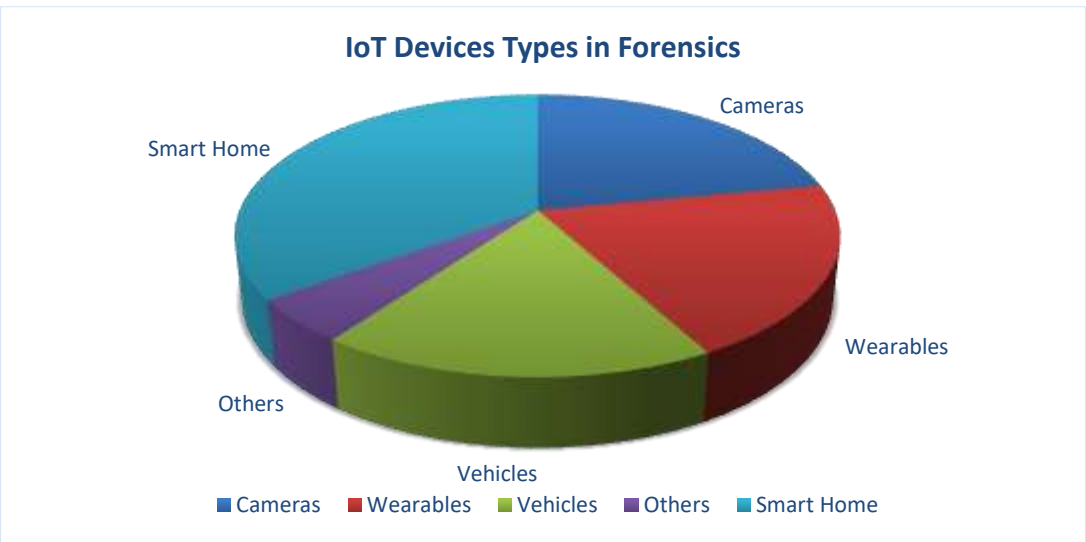


Source: Created by authors

2.1 Types of IoT devices relevant to crime scenes

IoT devices have made their way into crime scenes, with each device serving as either an evidence creator or an evidence investigator. Smart security cameras are capable of high-definition video and audio recordings, which are stamped in real-time, and sometimes provide cloud storage for video on remote servers. Wearable technologies - such as smartwatches and fitness trackers - track and record movement, heart rate, location, and time-stamped physical activity, providing investigators with critical details about a victim's or suspect's movements before, during, and after a crime occurred (Alanazi, 2025), (Alazab *et al.*, 2025). Smart home assistants (think Alexa or Google Home), smart thermostats, and bright lights all have histories of user interactions, ambient changes, and long-distance commands that can make or break alibis and timelines. It does not stop there, as vehicles equipped with IoT technologies at their core broaden the investigative trail of IoT even further, continuously logging states with respect to routes taken, speed records, points of entry and egress, and even communication transactions. If telematics is fitted to a car, it typically connects to a smartphone, leading to a rich source of evidentiary traces. Surveillance computers are capable of detecting motion and other variables, such as temperature and pressure, which can help capture data and transfer this information through drones. The Proportion of Distribution of categories of IoT devices found in cases is displayed in Figure 2.

Figure 2: Proportion of Distribution of IoT Device Categories Encountered in Cases



Source: Created by authors

2.2 How IoT devices collect, store, and transmit data

The IoT forensic value lies in having high-granularity data continuously and automatically gathered. Devices use a high number of sensors to record activities, interactions, and environmental states and process and store them locally or on cloud architecture. While there are many different positions that forensic investigators can find themselves in, crime scenes often only involve devices - most typically smartphones and computers, where they retrieve logs, communications history, geospatial information, and in some cases, environmental sensor readings either on the device itself or through the use of secure network connections. If it has recorded phonetic sounds for voice commands given to smart speakers, changes in room temperature, or passages read aloud from GPS trackers, it constitutes digital evidence. When using Wi-Fi, cellular, Bluetooth, Zigbee, or a proprietary radio network, data is transmitted over various protocols. As such, the presence of numerous standards for transmission can both aid and hinder investigations, as it requires forensic experts to be well-versed in extracting data from each device and interpreting the data accordingly (Khalil *et al.*, 2023). Although the timestamped logs and encrypted storage have significant roles in frustrating the data integrity, proprietary encryption and closed-source systems are tricky in retrieving and confirming these resources.

2.3 IoT data in crime scene context

IoT is useful in a criminal investigation since it is capable of tracking the actions and events preceding, accompanying and following a criminal act. Smart door locks, such as, can give an account of every entry and exit and can be mutually adjusted with other devices within a home and a timeline can be assembled of what occurred. Physiological usage of wearables can report an immediate rise in heart rate or movement and vehicle telematics can verify traveling to and attendance to certain locations. Environmental sensors are able to capture relevant contextual changes such as changes in temperature or humidity to give what scientists commonly call hard evidence to support the hypothesis of the sequencing and timing of crimes (Eyhab *et al.*, 2018). To process IoT evidence, evidence producers rely on the same procedures used by Murtha et al. (2008) to do so, which have the potential to retain chain of custody, assure data integrity, and support authenticity. The sophisticated forensic tools may visited, crack, and strip data on the devices and the on-cloud systems. It is a technique that uses software and algorithms to incorporate irrelevant data streams and searches patterns to detect the presence, motive, opportunity, or behaviour after a crime.

2.4 Facilitation of investigation through IoT

The possibility of implementing the IoT into inquiries generates amazing opportunities, the ones of accuracy and effectiveness, which we, perhaps, could not even

dream of. The IoT has the ability to alert and provide live feeds, so decisions can be made regardless of the raid or search (or emergency) operational decision and, consequently, the response time can be improved. The records of devices can be interrogated by investigatory personnel remotely, which is why direct contact with crime scenes is not required, and chances of contaminating evidence are minimal. The element of automation counteracts the element of human error or omission in the process by offering solutions in automated form since automated aspects of these systems include motion-activated video recording or triggering an alarm. Data about IoT tools can also assist in verifying or refuting statements of witnesses or suspects. As an example, scene description or truth claims are confirmed by GPS logs, sensors in the room, or communication logs. In multi-cases, data triangulation generates forensic verifiability that is often far greater than that corresponding to traditional evidence bases.

In fact, the opportunities of the Internet of Things (IoT) are unquestionable, but numerous obstacles to obtaining the evidences of such gadgets are manifold. Owned communication standards, a mixed range of equipment and advanced encryption algorithms that hinder easy access and retrieval of data that is beneath it. Furthermore, the privacy laws and the cross-border jurisdictional limits also drive the nightmares in cracking down on information, and as a result, the investigators often request device manufacturers or service providers to cooperate. In order to bring the truthfulness or inadmissibility of the evidence obtained through the IoT to a court of law, it is necessary to scrutinize the process of extracting, preserving, and authenticating evidence rigorously; otherwise, any breach of the chain will subject the product to suspicions of manipulation, falsification, or incompleteness (Altaha & Rahman, 2025). The proliferation of IoT sensors to conduct surveillance and gather data in great numbers also increases the chances of data breaches and mis-abuse of personal data and induces serious social and ethical concerns. The dilemma concerning the establishment of a balance between the requirements of the most important use of investigations and the needs of protection of ethics is also an old question that needs definite decisions and sound regulation. With the introduction of the IoT into the crime - scene investigation, the technological revolution has swept through all the spheres of the forensic practice: thousands of digital footprints are being recorded, examined, and reconstructed and Darling is able to work out proper timeline, recreate crime scene, and make a discovery of how a criminal activity takes place. Assigned the changing field of forensics, however, its practitioners must also address the technology change to make their practices consistent with the changes in data collection, security, and analytics without violating the law and integrity. Consequently, IoT is no longer an enthusiasm, value-added concept, but a strategic, premeditated component of the criminal investigation, and this generates a tricky overlap of technology and justice.

2.5 Applications of IoT in crime scene investigation

IoT has brought a whole new dimension in the sphere of crime-scene investigation and offered sufficient insights of online evidence, progressive monitoring variables and fragile forensics renewal. The burgeoning expansion of IoT devices into everyday life means that, nowadays, both in a crime scene and outside, while on the run, you often leave behind traces of yourself via innovative technology. These devices are recognised today based on their utility as primary sources of evidence identified with forensic significance, rather than as secondary sources. They may be employed for evidence collection, scene reconstruction, real-time surveillance, geolocation tracking, and data forensics to generate information that might otherwise prove elusive. Applications associated with using IoT evidence in real crime investigations are listed in Table 1.

Table 1: Applications of IoT Evidence in Real Crime Investigations

Investigation Type	IoT Device Used	Forensic Technique	Outcome Achieved
Homicide	Fitness tracker, smart lock	Timeline reconstruction	Accurate time of death established
Burglary	Surveillance cameras	Video review	Suspect identified via footage
Hit-and-run accident	Vehicle telematics	Route mapping	Suspect location confirmed
Domestic violence	Smart home assistant	Audio log analysis	Threats corroborated
Fire/arson	Environmental sensors, drones	Mapping changes	Cause and sequence validated

2.6 Evidence collection and digital trace retrieval

The fundamental value proposition that IoT contributes to forensic science is the simulated digital traces of actions, interactions, and environmental states that the IoT system is designed to create and store. Law enforcement agencies often access the data stored in, or transmitted by, smart home devices, wearables such as fitness trackers or smartwatches, networked cars, and network security cameras. This includes entry and exit logs, voice activity, biometric data, motion paths, and environmental sensor data, all of which are timestamped. For instance, a hack of a smart home can be replayed by pulling data from when a door was locked or unlocked, from when an alarm was activated or deactivated, or from when internal video was activated or deactivated, or when lights and thermostats were set (Atlam *et al.*, 2024). Wearable technology could include access to location histories, heart rates and physical activity - providing a chronology of movements of a victim or suspect and potentially linking one to a homicide. In the context of IoT crime scene investigation, forensic experts retrieve and verify IoT evidence using specialised software and extraction tools, which are typically provided by vendors or developed by independent laboratories. Cloud: Cloud access to data is often a big challenge- sometimes

requires warrants or intervention by the cloud provider but the redundancy nature of cloud-based infrastructures assists in maintaining data safety in case of the loss of machines. Chain-of-custody processes require that forensic integrity is unviolated and that provenance concerning any recovered data should be strictly proven to make it admissible in a legal courtroom.

2.7 Crime scene reconstruction and pattern recognition

Such a capability allows accurately recreating the acts of a criminal, which was impossible to do before the development of IoT devices. Industrial surveillance (especially during crises) involves video and audio recordings that allow investigators to compile minute by minute timelines based on camera-timestamp (Atlam *et al.*, 2020). Sensors of the environment, e.g., movement sensors, temperature sensors, humidity sensors, etc., enable investigators to offer supportive or refuted testimony by the witnesses, retrace the tracks of a suspect, and draw relationships or causal connections under certain situations. The use of artificial intelligence and machine-learning algorithms to work with the huge, multifaceted volumes of data produced by IoT devices has become more common.

These technologies combine different data streams to bring out patterns and anomalies and possible causes. An example is arson, a sensor reading showing a changes into heat at a particular time as a motion detector in a certain room report, after cross-referencing sensor data with that of security-cams will locate the point of origin and time of the fire. AI-based reconstruction helps to combine the data of heterogeneous sources of the IoT into the three-dimensional models of the surroundings where the crime scene is, probable situations, and extrapolate stories using the evidence. As a result, the timelines of investigations are also accelerated, and hypothesis testing is reinforced, and many breakthroughs tend to be substantial.

2.8 Surveillance, monitoring, and predictive analytics

What appears to be the most consequential IoT touchpoint in the crime-scene investigation model is the ability to surveil and monitor in real-time. Smart security systems use motion sensors, cameras and alarm systems that automatically activate once the extra movement is realized, thus reporting both on-site staff and the external responders. Voice-controlled aides can pick up someone speaking or giving commands and attach the audio directly to case files. Geolocation tracking of vehicles or wearables is essential for placing suspects or victims at a specific location, contradicting or verifying an alibi, and tracking mobility before, during, and after a crime (Baho & Abawajy, 2023), (Brotsis *et al.*, 2019).

Advanced predictive analysis utilises historical IoT data to identify trends that may be associated with opportunistic crime or predict potential threats. For example, security

systems interfacing with crime databases may be programmed to send out a warning when a suspect, whose face has been recognised, enters an area of coverage, or when motion detectors detect unusual activity in a time frame statistically associated with home invasion. These analytical practices are all mooted on sound data integration and privacy-awareness, and attempt to balance investigative efficiency with the ethical custodianship.

2.9 Data forensics: Extraction, analysis, and challenges

Technical performance and forensic demands usually demand that experts have sophisticated skills of retrieving and analyzing data transmitted by IoT devices. The variety of the operating systems, the formats of encryptions, and the models of cloud connections of the devices are mind-blowing. Through the rudimentary custom-made boxes to business fitness trackers, the forensic investigators would have to establish a lucid grasp of the framework of the creation and its work-specifics (Conti *et al.*, 2018). Extraction tools are able to fetch the devices physically (USB ports, SD cards, etc.) or in a remote manner (wireless, API in the clouds and the cloud).

Forensic process demands the integrity of the data, an accurate account of the process of collection in the modern logs and the assurance of its reproducibility. The biggest complication of this fact is that either the suspects or remote operators can either erase evidence or distort it. The methods of preservation (live, quick, backup imaging, etc.) become important. vetting of metadata in form of checking the metadata and validating its provenance is also supported by a comparison of the metadata, timestamps, device identifiers, and access logs (Conti *et al.*, 2017). Legal admissibility, along with privacy concerns, makes forensic examination of IoT data very challenging. This requires the courts to be explicit about requiring unbroken, scientific chains of custody. At the same time, technical experts must describe what happens to the device, how the data is generated, and what protocol is followed throughout the analysis process. When some devices store information in foreign territory data, e.g., cloud storage (which is a foreign country), or require business assistance to decrypt data, jurisdiction is questioned.

3.0 Integrating IoT with Traditional Evidence and Case Studies

Traditional forms of evidence (testimonial, physical or biological) are augmented with IoT information; IoT information is rarely found alone. IoT evidence is regularly cited alongside fingerprints, DNA evidence from the crime scene, witness testimony, and other material traces. Case studies highlight specific examples where IoT evidence has, beyond a reasonable doubt, actually changed the outcome of a criminal investigation - such as when a murder victim's case was contradicted by their fitness watch (as shown, below, in an

example report), or a break-in was solved by aligning security footage with vehicle telematics logs. IoT device logs can reveal unauthorised entry, remote control activities, or unusual usage patterns during fraud and cybercrime investigations. Time of death disputes have even been settled using environmental sensors (which have indicated changes in room temperature), and intelligent assistants have provided damning recordings of voices.

In one notorious murder case you might remember, it was IoT devices that broke the case wide open. A voice assistant, security cameras, bright lighting, climate control, and the victim's own wearable device: The crime scene was not just a single location, but a smart home. The responders obtained voice logs from the assistant when an abnormal order to dim the lights and play music was given a few minutes before the approximate time of death. The use of security cameras showed how the intruder entered and exited the building, as well as how the victim and the perpetrator entered and exited the location (Kandwal, 2024).

The device recorded an accelerometer-detected heart rate spike and subsequent complete quiescence, all of which occurred at an approximate forensic time-of-death (TOD) estimate. Integrating such a wide range of sources, the forensic analysts are put back to a consistent chronology of the events, including how the suspect approached, how he or she entered the premises, how the ambient conditions were modified, how the victim reacted to the situation, and how the movement in the event came to a stop. An in-depth account is created based on CCTV cameras, tapes, and biological data. Throughout the situations when proprietors of investigation have to face challenges of cloud-based ciphering and asynchronous synchronization of the gadgets, they maintain the chain of custody so hard and safeguard the integrity of the evidence, allowing the prosecutors to win their case. The case study focuses on the point where IoT data can be used to support a physical evidence, bolster a witness testimony, and, overall, improves the evidence strength in a forensic setting. As the IoT is potential to create huge dividends, its functionality in crime-scene investigation is still riddled with considerable issues.

The lack of device homogeneity, proprietary protocols, and the fast development of hardware makes the tool building process and the creation of the investigative protocols more complicated. Even such functions as encryption and security, which are meant to shield the users, are also meant to limit the ability to access the forensic scope, that is, collaboration is required on behalf of the manufacturers or the police force. Since changes or errors in the firmware of Internet of Things (IoT) gadgets can lead to the quality of information, investigators should address the integrity and reliability of the IoT evidence. IoT Research Secret beneath Privacy and Ethical Concerns. The gadgets capture treasure troves of personal data which is in no way relevant to the allegation of crime, and the issues of scope and relevance arise.

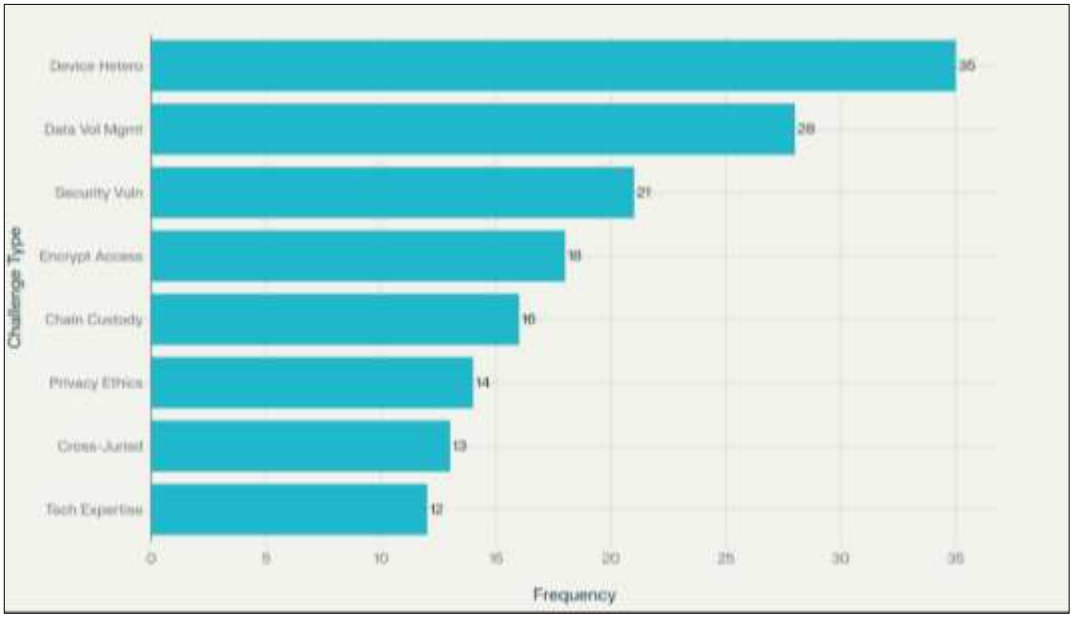
Additional factor of this threat of mass gathering of information against civil liberties needs to be amortised with the privacy rights to promote greater vigilance in the investigational necessity of access. It needs standardised rules and open procedures to protect against abuse and uphold trust in the part of the public. In the future, new technologies like blockchain-based authentication and edge computing will increase the reliability and analytics of the IoT forensics. The adoption of blockchain provides enduring records of access and transfer of data to individual data and additional chains of custody that cannot be tampered with. It enables decentralised analysis at the point of use of the device therefore minimizing the bottlenecks of transmitted information and the state of the original evidence is preserved. Artificial intelligence will develop IoT forensics, making it possible to automate analysis and refine pattern discovery therefore making possible new types of predictive policing.

Nevertheless, with an improved technology, there is a need to make adjustments - forensic scientists, lawyers, and administrators will have to come up with procedures that preserve the integrity of the evidence that the techniques produce but must not overstep the line to the extreme of infringing upon the ethical standards (Fagbola & Venter, 2022). The use of the Internet of Things to investigate a crime scene is, quite literally, a game changer due to the increased scope, speed, and accuracy of the forensic field. The inter-relationship of the current environments allows scholars to obtain a wide range of digital data and analytics functions on an unparalleled scope. In the case of the combination of AI and specific software, the IoT evidence allows reconstructing the actual events, improving surveillance and tracking, and even performing high-grade forensic research. Following the issue of security, privacy and interoperability, it is still necessary that a lot of research and legislative legislation be done to realise their full capabilities. The use of the IoT technology as a justice supplement justifiably supports the current and future examination of crime scenes and introduces technical resourcefulness and forensic wisdom.

4.0 Legal and Ethical Challenges in Using IoT for Crime Scene Investigation

The rise of IoT in individuals, businesses, and governmental settings in a tragic growth has significantly altered the crime scene detection method. Nevertheless, it has also produced numerous complicated legal and ethical dilemmas which are to be considered by forensic professionals, police, and judicial systems. The majority of these issues are saturated with privacy, data protection, admissibility, cross-jurisdictional matters, and evidence manipulation are its likely consequences, with a considerable implication to the overall trust of the masses and the quality of justice. Figure 3 Stacked bar chart proves the presence of legal and technical hindrances to the IoT forensics, as indicated by (2025).

Figure 3: Stacked Bar Chart Depicting Reported Legal and Technical Obstacles in IoT Forensic Investigations (2025)



Source: Created by authors

4.1 Privacy concerns

Privacy is the key issue in the legal and ethical dilemma of IoT. The agency that has been proposed by the exhaustive, granular information gathering offered by IoT devices makes people apprehensive of the procivation and exploitation of the highly personal data. Connected cars, wearables, home security systems, smart speakers are all related to Alexa, Echo, and Google Home that store sensitive user related audio files, geolocation history, biometric scans and behavioural patterns. Much of this information lies beyond the criminal event, such as events in the lifetime of a person, his or her habits, and relationships. Legally, the boundaries of what is good evidence gathering is blurred. This implies that the investigators must be careful enough to prevent the violation of the GDPR in Europe or any other mechanisms limiting the processing of the personal information based on the scope, time, and purpose (Ghasemi & Mahmoudi, 2024).

When the collection is made with lenses or the collection does not meet the specified criteria, the same results in a threat of violating constitutional protection. It may also have consequences on the admissibility of electronic evidence in court and integrity. At a more philosophical level, waging such an ethical battle will continuously cause a conflict

between the necessity of minimizing the regulations of the investigation in order to achieve prosecution and avoid violating rights to the minimum. A significant surveillance provided by the IoT sensors - many of which may be placed without constant agreement with the user - raises the issue of intrusion and a decrease in the privacy. Transparency, minimization, secure and properly laid down protocols, are required to ensure civil liberties are retained and to reassure the society.

4.2 Admissibility of IoT data in court

The concept that lies between forensic potential and forensic utility is admissibility. The evidence provided by the Internet of Things should address high standards, i.e., authenticity, integrity, reliability and relevance. Judges are looking at the digital footprints to see if there has been tampering in handling or interference in handling or the chain of custody of the same has been compromised. Evidence derived from smart devices is often disputed on technical grounds - time synchronisation, device identity, encryption, and access logs must be proven and justified by experts. Legal precedents continue to evolve - for example, who owns data on IoT devices and in the cloud?

In what circumstances could law enforcement compel manufacturers or users of a device to disclose information? What dynamics apply to data derived from collaborative spaces? Each has interesting implications for admissibility now and for how this will be practised in the future. In other criminal cases, the difference between denial and exclusion can hinge on minor issues, such as broken warrant protocols, gaps in the chain of custody, or the inability to determine the authenticity of files extracted from a device. Forensic examiners are expected by law to do more than perform technical work; they must possess a broad knowledge of procedural law and courtroom testimony (Granjal *et al.*, 2015).

4.3 Evidence tampering and data integrity

While physical evidence is less so, digital artefacts from persisting IoT devices are curious in that they can be modified, deleted, and remotely modified. Additionally, many devices can be remotely updated, factory reset, or wiped, which criminals can exploit to hinder investigations. Added to this danger is the fact that cloud storage allows any piece of information to be changed or erased, so long as someone can access the account.

Lastly, live imaging, isolation devices, and hash values are preservation measures that are required to ensure the purity and authenticity of IoT forensic data. Investigators should be able to adapt fast in order to secure data that might evolve fast, record their activity as well as adhere to definite procedures to retrieve them. At the same time, in case the threat concerns undetectable tampering or spoofing, the timely, proficient, and technical examination should be appropriate, and the solid solution to such instances in court.

4.4 Cross-jurisdictional legal complexities

Most IoT devices save their information on the servers outside the territorial grounds of the crime scene or connect with cloud applications that are governed in laws of another country. It is a maze of legal hurdles that investigators have to go through before getting access to it because the standard of data protection, privacy, and cooperation between law enforcers differ greatly across the country (Grispos *et al.*, 2024). Intercountry requests of electronic evidence undergo a complex interconnection of international treaties, mutual legal assistance treaties and national statutory obligations. Jurisdictional gray areas may turn the chain of evidence into a snarl, slow down, or even jeopardise criminal actions. In the meantime, international organizations are making efforts to unify access to data by agencies but investigators must remain wary of the need to follow electronic evidence in transnational borders. Nevertheless, the lack of constructive cooperation and confidence among all the agencies would render the effectiveness of forensic outcomes weak, which is not favourable to anyone, since we are all heading towards the objective of a safe and secure world.

4.5 Ethical issues in forensic use of IoT data

Although the process of gathering evidence will meet the legal requirement, the ethical concerns of IoT in crime scene investigation may be questionable. This implies that the privacy privileges of the suspects, victims, and any other innocent individuals whose information are incidentally picked by the investigators during the search of the suspects are safeguarded. Since algorithms and computer systems have to process massive IoT data to determine the correlations and patterns, the probability of discrimination or an unjust implication might be even higher (Mahmood *et al.*, 2024), (Mahmud *et al.*, 2017).

It is important to avoid bias, omit or falsify data plus to avoid human control over the findings given by AI, its examination and analysis. Such ethical requirements encompass the adherence to transparency when conducting an investigation, informed consent to use the data (where applicable), and fair proportionality in evidence acquisition. There should be a clear account of the kinds of decisions made, the reasoning behind such decisions, and the precautions taken at each point in time during the investigation process by the forensic experts.

4.6 Regulatory frameworks and the path forward

The legal and ethical issues surrounding the investigation of IoT crime scenes require a more inclusive regulatory framework, sustained with detailed legislation, like the one Canada has recently implemented, prior to managing the problem. It must contain approved spheres of data gathering, technical requirements to get and keep evidence,

legislative needs to what is admissible, and strategies to facilitate among departments. We also need constant learning in this dynamic world of technology and the cross-disciplinary discourse along with constant oversight of best practices. The solutions (blockchain-based custody chains, state-of-the-art Encryption to allow edge computing to process data in devices) would make it safer and minimize risks that may occur.

Therefore, the policymakers should consider the positive aspects of technological advancement against the relative value of privacy, equity, and accountability (Yaqoob *et al.*, 2019). Finally, using the appropriate leveraging of the IoT technology in the forensic practice, the process of an investigation and the efficiency of the investigation can be progressively improved, as well as the final verdict of a court. However, it will only succeed with the diligence, vigilance, and moral compass of police, forensic professionals, and the criminal justice system as a whole. The path is one of balance - a balance between innovation and caution, a balance between safety and personal freedoms, and a balance between the science of forensics and the science of social policy.

5.0 Challenges and Limitations in IoT-Enabled Crime Scene Investigation

The types of technologies that were once exceedingly expensive and unavailable to forensic science at all due to their systemic inapplicability have become, almost by revolution, and admittedly at a grudgingly high cost, available at the crime scenes, in a range of Internet of Things (IoT) technologies. With the growth of the use of IoT devices spread everywhere due to its implementation in smarter homes, wearable data collection technology, mass usage in connected automobiles and the utilization of IoT to collect evidence in the view of the general population, the process of retrieving, verifying and retrieving evidence that is derived by the internet of things will grow exponentially. Abstract: The review is a summary of the best issues and challenges that can impact forensic interaction with the evidence of IoT devices.

5.1 Device heterogeneity and proprietary standards

Another characteristic of an IoT environment, which is of the utmost importance, is the large degree of heterogeneity of devices that include not only other brands but can also feature diverse hardware architectures, operating systems, data formats, and communication protocols. Every vendor would make the establishment of a standard forensic tooling and processes difficult by the use of proprietary software, algorithms, or specific encryption mechanisms, or custom data storage facilities (Islam *et al.*, 2019). Alternatively, researchers normally use the support of the vendor or reverse engineering to develop insight on information at rest consequently having a minute-by-minute knowledge of the operational

model of each device. This fragmentation does not only complicate the ease with which evidence can be collected but is usually error prone and procrastinates the reliability and reproducibility which admissibility to legal allegation necessitates.

5.2 Data volume, management and interoperability

The amount of data that is produced by IoT enabled devices is enormous making it difficult to warehouse, analyze and retrieve this data. Crime scenes can give rise to large amounts of data, dozens of sensors, cameras, Internet of Things (IoT) devices - even gigabytes or terabytes of digital evidence per case. Data should be both managed and mapped on a regular basis, but this is actually a challenge as interoperability between platforms and devices does not exist. It is time consuming to keep a brochure that has merely manual correlation. Meanwhile, an automated review software might overlook links that can be valuable to your analysis or will cause enterprise analysis biasness (Islam *et al.*, 2019). In order to handle this data explosion and derive operational intelligence out of it without undermining the veracity of the data, forensics professionals need sophisticated AI-driven solutions and high-quality standardisation.

5.3 Security vulnerabilities and data integrity risks

When a cybercriminal locates a vulnerability within the system (a default credential, unpatched firmware, or an insecure networking protocol) he or she takes advantage of the vulnerability. They may make IoT devices become repeat victimised. Actually, successful attacks may lead to the loss of the data, data maneuvering, or the addition of planted evidences- threats which carry far reaching forensic consequences. Remote management (factory resets and remote wiping) can also be used against a victim by an attacker in order to destroy or modify important evidence before the investigators can get evidence of it (Kaushik *et al.*, 2023). Quick incident response, forensic imaging, and cryptographic verification (e.g. the digital hashes) are necessary to ensure the integrity of the data but volatility and accessibility have been constant and are an apparent threat.

5.4 Encryption and access barriers

Expanded use of more powerful encryption - particularly with consumer IoT devices - is a future guarantee of privacy to the users, and a wildfire that renders lawful forensic investigation unfeasible. Cashing in on such a degree of seclusion would imply that police officers would get shut out of the essential log on gadgets, encrypted (cloud-depicted) repositories, or company carrier messages (Kumar *et al.*, 2021). The lawful authority to force decryption can also be a humdrum problem, according to the jurisdiction and the place where the information is stored. Collaboration between the manufacturer

helping to perform an analysis of the brute force key is time-saving, and the brute force decryption is not always possible within the resource and time constraint of a criminal investigation.

5.5 Chain of custody and admissibility challenges

Evidence that has a plausible chain of custody is an important milestone towards the admissibility of evidence in a court of law. On this basis of volatility, remoteness and amendability, IoT-derived data is exceptionally prone to substantiation-grounded challenges on this or other grounds (Mahmood *et al.*, 2024). Seizure, storage and any alteration made on the same along with details of access logs and the loopholes should be documented in detail. Metadata, timestamps, and device identifiers have to be reviewed which can be utilized to counter charges of manipulation. Inadequate documentation or malfunction of programs may result in omission of evidence, a disadvantage to forensic opinions, and finally, unsuccessful prosecution.

5.6 Privacy, ethics and scope creep

Privacy IoT can be viewed as the most privacy intrusive in instances where forensic investigators can use the technology to gather very personal, in most cases unrelated information about mobile targets on the scene- and in some cases, even none targets on the scene. The new regulations regarding privacy stipulate what investigators can do to ensure that this process does not infringe upon the privacy of the subjects involved, thus this is one area that investigators have to be careful about (Mahmoud *et al.*, 2015), (Mazhar *et al.*, 2022). Too much forensic collection may be a crime against civil liberties; every line of inquiry has to be carried out within the doctrine of minimisation, consent (where feasible) and open procedures.

5.7 Cross-jurisdictional and regulatory issues

Since the majority of internet of things devices archive information in the clouds located in a different state, but, not in the same territory where the crime is carried out (also typically a connected mobile phone), interwoven problems of legal accessibility, cooperation, and sovereignty are raised (Mishra & Pandya, 2021), (Mukhtar *et al.*, 2023). Acquiring international evidence may be cumbersome, time consuming and full of bureaucracy and the fact that there are varying laws governing privacy and data protection - complicates the process of investigation and prosecution. Reforms aimed at aligning the legal process and investing in vehicles to make international collaboration possible are all needed, but the latter change reluctantly at best.

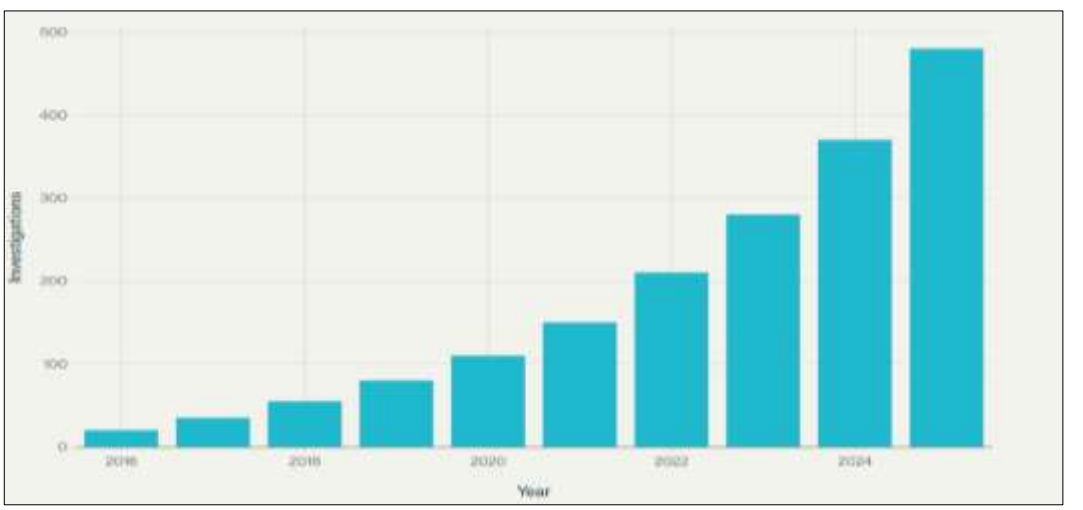
5.8 Technical expertise and resource constraints

Overall, IoT forensics is a constantly changing field that requires constant practice and change. The majority, or even all, the law enforcement agencies have gaps in skills, underutilization of sophisticated analytical tools, or resource limitations that hinder management of the IoT evidence on time and in the most adequate manner. The promising outlooks are professional training, interdisciplinary interaction, and the investment in specific products, which allow staying up to date in the stream of the technological flow and deliver good forensic deliverables. The ability of the IoT technologies to impact on the paradigm shift in the work of defining a crime scene cannot be denied, yet the forensic practitioners still have numerous technical, legal, organisational and ethical issues (Nawir *et al.*, 2016). The tools needed to overcome these limitations will be on-going research, involvement of the stakeholders and organisation scaffolding of loose yet solid investigation guidelines. Such problems ought to be conquered before total utilization of the IoT evidence in pursuit of truth and justice.

6.0 Future Trends and Innovations in IoT-Enabled Crime Scene Investigation

With the ongoing revolutionization of forensic science through the Internet of things tools and techniques of conducting criminal scene investigations and their data sources will change drastically, as the tools and techniques grow more innovative, data-powered, and more autonomous.

Figure 4: Annual Increasing Trend in IoT-based Crime Scene Investigations (2016-2025)



Source: Created by authors

These represent only some of the profound future trends and developments that are coming into play as the law enforcement and forensic community tries to keep up with this revolution (Nieto *et al.*, 2017). These developments open up the possibility of developing paradigm shifts, not mere additions to the capabilities of discovery, analysis and presentation of digital evidence in current paradigms. But going forward into the future of IoT-enabled crime scene investigation it is evident that, innovative forensic ecosystems is bound to achieve its potentials with constant advancement in technology, interdisciplinary studies and reforms of laws as they keep up with the changing technologies. Additionally, IoT-based crime scene investigations have experienced upward growth every year since 2016, as depicted in Figure 4 (2016-2025).

6.1 Artificial intelligence and machine learning for IoT forensics

Machine Learning and Artificial Intelligence (AI) are poised to change the forensic example from applications to IoT vastly. These technologies offer advanced pattern recognition and predictive analytics, assisting in real-time decision-making on the massive datasets produced by connected devices. Most evidence extraction tasks will be automated with AI-based solutions that intelligently review millions of event logs and connect device activity across multiple systems (Edewede *et al.*, 2013), (Perumal *et al.*, 2015). The authors provide a practical example, illustrating how investigators can apply machine learning models to identify behavioural patterns in smart home data and detect anomalies that may indicate potential criminal involvement or exclude false positive data.

Leaving aside the details, the form of temporal and spatial analytics will be critical in reconstructing a crime scene, where AI will infer probable sequences of events from incomplete, noisy or fairly corrupted information. As increasing volumes of data become too large for humans to review, AI will be crucial in accelerating investigations and minimising the risk of human error or bias (Garcia Avila *et al.*, 2024). Additionally, explainable AI-a field that pursues transparency and accountability -will ensure that forensic insights drawn from automated systems are scientifically sound and judicially sustainable. Interpretability will be more critical than ever in making machine learning findings readable to people, and the courts will demand the same in future studies.

6.2 Blockchain and distributed ledger technology for chain of custody

Digital evidence integrity is crucial in forensic practice, especially for traces that are potentially vulnerable to tampering, deletion, or unauthorised access, such as those arising from IoT. Evidence and chain of custody are the domains, where blockchain (distributed ledger technologies) is an actual eye opener. The blockchain produces the unalterable time-stamped records of every access, change and transfer, which removes

suspicion and reinforces the legitimacy of the forensic process. Whenever an IoT device communicates, it can automatically store the data in the blockchain storage facility and can be tracked and confirmed in the future, which will revolutionize crime scene investigation in the future. Not just the investigators enjoy the benefits of such device since this also allows defence lawyers and courts, an objective and automated history of evidence processing through the whole chain of custody, starting with the original to courtroom presentation (Rudrakar *et al.*, 2025). Distributed ledgers will contain privacy-by-design, which will balance transparency and confidentiality, avoiding the unnecessary leakage of data, on the one hand, and preserving the rigor of evidence, on the other. Actual crimes will involve forensic scientists, cryptographers and jurists collaborating in various fields in order to implement blockchain protocols in actual crimes. The ultimate factor that will see these advances being converted by theory to fact will be scalability, interoperability and regulatory validation.

6.3 Edge computing and real-time data analysis

The necessity to process information locally, at the point of origin, i.e. edge computing, rather than at the center of the cloud-based servers, forms a major evolutionary leap forward in the field of forensic science. Evidence bytes will also be digested by edge analytics at a crime scene, and this will provide the ability to preserve evidence as soon as it is produced by the IoT device, to respond to alerts more quickly, and reduce the chances of data loss or manipulation during transit. Using edge computing, motion logs, sensor data, and video streams can be processed on site giving the investigator the capability to react to real-time events. For example, an intelligent security camera may recognise if some form of tampering is taking place, provide immediate alerts, and begin secure evidence archival locally before any information is sent offsite (Francesco & Eoghan, 2019). Decentralisation also improves privacy, stops bandwidth bottlenecks, and makes important information available when things get difficult and network breakdowns occur. Forensic triage-sorting (prioritising, scoring, sifting, ranking)-based on relevance and volatility, at the device level, will also be possible, leveraging edge computing. As AI-powered devices become more powerful, investigators can expect more robust preliminary analysis, reducing the time and energy spent transferring terabytes of information to a central lab.

6.4 Next-generation device interoperability and standardisation

The lack of uniform standards across IoT devices has long been a barrier to forensic advancement. The future promises an increase in interoperability research and development as manufacturers, standards organisations, and law enforcement all act in concert. Forensic APIs, protocols and formats will become the new standard, and plug-and-play evidence

extraction will be the new norm. At the same time, the need for device-specific reverse engineering or dependency on commercial solutions will begin to lessen. Converged requirements will also drive the development of more robust forensic kits in the field that can reach out to and extract data from almost any IoT device (Sharma *et al.*, 2023). This will give smaller agencies access to a higher level of forensics and even out the level of investigation between agencies. Also, the standards of the security, auditability, and authenticity of the evidence embedded in every design of an IoT device will be taken into account by the evolving regulatory environment. Based on the anticipation of tighter legal obligations to access and preserve data, manufacturers will be compelled to integrate forensic readiness and compliance capabilities into their offerings.

6.5 Privacy-enhancing technologies and ethical innovations

This aspect of the application of privacy-enhancing technologies (PETs) to IoT forensics will form a priority consideration during the future crime scene investigation. Such data sent by devices can be selectively accessed with the help of so-called privacy-enhancing technologies (PETs), i.e. different privacy, secure multi-party computation, and homomorphic encryption, so irrelevant personal information will never have to be divulged, unless in a forensic perspective. These technologies would resolve the ethical issues of the scope creep and data minimisation which may enable the investigator to gather sensitive or irrelevant data on innocent people unintentionally (Silva *et al.*, 2025).

The Privacy Dashboards and Dynamic Consent Frameworks, and High-Granularity Access Control, will ease the process of monitoring and managing the utilization of IoT data, which will restore the confidence and acceptance of the Social Acceptance of Intelligent Crime Scene Investigation among people. The experts in the field of forensics will need periodical and continuing training regarding issues of data ethics, digital rights as well as new privacy and data protective technologies. This training will entail liaising with legal researchers and civil society players to come up with open and culturally attentive protocols of evidence.

6.6 Incorporation of new sensor modalities and multimodal analytics

Far in the future, crime scenes will consist of more and more modalities of the new IoT sensors in the environmental, physiological, biometric, acoustic, and chemical sensors. It will give much more profound, situational insight into criminal activity. The correlation of data of several sensor modalities will provide multimodal analytics, which will allow reconstructing events and profiling person-of-interest behaviour. As an example, the physical fight is not only recorded on audio and video, but also on sensing the environment that will indicate the temperature level, air quality and room presence.

Integrated timeline Stress markers, physical activity, and biometrics wearables would provide colour to a list of activities (Sivanathan, 2020). With all these forms of data streams, investigators will merge them to form digital pieces of evidence and employ the most recent visualisation and reporting systems. Forensic styles will be not static but dynamic, situational analytics, deriving meaning out of incomplete, uncertain or incongruent information with certainty and integrity as sensor data transitions to finer and richer streams. Interaction with Advanced Robotics and Autonomous Forensic Agents.

6.7 Integration with advanced robotics and autonomous forensic agents

Even further collaboration between forensic professions and robotics and autonomous agents will happen. This will allow the drone sensors with IoT to allow the drone to perform an aerial survey, map a layer, and take visual evidence that is inaccessible to the human inspectors or so dangerous that it is impossible to reach it. Crime scenes will be monitored by the use of a mobile robotic agent fitted with environmental and chemical sensors which will monitor and detect anomaly in details of volatile evidence within minutes. The loading of AI-based-based algorithms in the field by degenerative forensic agents can generate initial hypothesis testing and transfer the outcomes to remote forensic agents. Their ability not to become exhausted, not to err, and to work 24/7 could speed up the first impression of the scenes and provide the opportunity to recreate complicated scenarios (Sivaraman *et al.*, 2015). Human analysts will be at the forefront to ensure that such innovations are aligned to the objectives of investigation besides the ethics framework.

6.8 Legal frameworks, international collaboration and policy innovations

The dynamic character of the IoT-enabled forensics at the international level will require the legal reformation. The standards of progress will include regimes of legal access, transport of international data and a privacy shield. Leveraged, timely collaboration of the involved agencies will not only have to be conquered, but the aspect of international co-op pacts and treaty frameworks will change as well. Automated legal procedures will boost simplified procedures of the warrant requests, multiple party request of data and the conflict resolution procedures concerning the evidence management/integrity (Brotsis *et al.*, 2023). The state of what is right and wrong in the eyes of people and the freedom of individuals will be brought under the control of regulators since the technologies are evolving at a speed as blistering as light.

The short-term outlook of unparalleled adjustment in IoT-driven criminal investigations, empirically informed interdisciplinary practice, and reactive regulation. Innovations in AI and blockchain, edge computing, device interoperability, privacy-saving technology, sensor modalities, robotics, and legislation will intersect and become new

responsive and innovative, ethically answerable forensic systems. Subsequently, the investigators will be required to continue their toes-perpetually sharpening their skills and processes to address the requirements that are set forth by the quantity of data, variety of tools, protection, personal privacy, and legal complexities.

This implies the need to make education, research, and policy to become resilient, transparent, and accountable to the citizens in response to evolving technologies that can make crime scene investigations more resilient (Weber, 2010). IoT devices are not merely used but used as investigative technology in yielding digital forensic data that will likely form the future combining human-driven intelligence to seek vengeance, to tell the truth, and to safeguard the digital era society.

7.0 Conclusion

The constantly growing trend on Internet of Things (IoT) technologies in the field of forensic science has significantly transformed the view and context of the crime scene investigation to provide the degree of particularity, scope and velocity of evidences recovery, reconstruction and analysis on a way that would be practically impossible in an ideal world. The employed network of smart devices, such as wearable medical devices and environmental sensors, video surveillance camera, and smart cars, now present investigators with enormous amounts of digital evidence to complement contextual information and produce sure findings regarding the use of forensic methods.

Nevertheless, even achieving the full potential of IoT-based forensics can only be realised in case a wide range of extremely challenging technical, legal and ethical issues, including heterogeneity of devices, encryption concerns, data management problems, privacy issues and cross-jurisdictional access challenges are overcome. These gaps will be important to address through the implementation of new technologies, including artificial intelligence, authentication using blockchain, edge computing, privacy-enhancing technologies, and standardisation protocols to ensure data integrity and allow forensic results to be trusted.

Through the coordination of all the disciplines engaged, and by re-engineering our learning model to these emerging challenges that come as a result of the evolution of crime, of technology, and the interaction of the two, we will be nimble, agile, responsive, and ethical. The actual future of the IoT forensic science lies now in a real manner of incorporating the technological advancement and the concepts of justice to present more precise, powerful, and confident means to find out the truth in the rapidly altered digital world.

References

Abomhara, M. & Koien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility, 4*(1), 65-88.

Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A. & Abdulrahman, A. G. (2024). IoT forensics: Current perspectives and future directions. *Sensors*, *24*(16), 5210. Retrieved from https://doi.org/10.3390/s24165210

Alanazi, A. (2025). Intelligent IoT forensics: Secure evidence acquisition and autonomous intrusion detection. *International Journal of Innovative Research and Scientific Studies, 8*(5), 1167-1181. Retrieved https://doi.org/10.53894/ijirss.v8i5.9078

Alazab, A., Khraisat, A. & Singh, S. (2025). A review on the internet of things (IoT) forensics: Challenges, techniques, and evaluation of digital forensic tools. Retrieved from https://doi.org/10.5772/intechopen.109840

Al-Hussaeni, K., Brits, J., Praveen, M., Yaqoob, A. & Karamitsos, I. (2023). A review of internet of things (IoT) forensics frameworks and models. Retrieved from https://doi.org/10.1007/978-3-031-30694-5_37

Al-Masri, E., Bai, Y. & Li, J. (2018). A fog-based digital forensics investigation framework for IoT systems. Retrieved from https://doi.org/10.1109/SmartCloud.2018.00040

Altaha, S. & Rahman, M. M. (2025). Internet of things forensic: Contemporary issues, challenges, and future research directions. *Bulletin of Electrical Engineering and Informatics, 14*, 2735–2751. Retrieved from https://doi.org/10.11591/eei.v14i4.8716

Atlam, H. F., Ekuri, N., Azad, M. A. & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics, 13*(17), 3568. Retrieved from https://doi.org/10.3390/electronics13173568

Atlam, H. F., Hemdan, E. E., Alenezi, A., Alassafi, M., & Wills, G. (2020). Internet of Things forensics: A review. *Internet of Things, 11*, Article 100220. Retrieved from https://doi.org/10.1016/j.iot.2020.100220

Avila, R. G., Miller, F. & Iyengar, S. (2024). Current challenges in IoT security and forensics: Strategies for a secure connected future. Retrieved from https://doi.org/10.5772/intechopen.1007766

Baho, S. A., & Abawajy, J. (2023). Analysis of Consumer IoT Device Vulnerability Quantification Frameworks. *Electronics*, *12*(5), 1176. Retrieved from https://doi.org/10.3390/electronics12051176

Brotsis, S., Grammatikakis, K. P., Kavallieros, D., Mazilu, A. I., Kolokotronis, N., Limniotis, K., & Vassilakis, C. (2023). Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems. *Internet of Things, 24*, Article 100968. Retrieved from https://doi.org/10.1016/j.iot.2023.100968

Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavue, C. (2019). Blockchain solutions for forensic evidence preservation in IoT environments. *Proceedings of the 2019 IEEE Conference on Network Softwarization*, 110–114.

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. Retrieved from https://doi.org/10.1016/j.future.2016.11.031

Fagbola, F. I. & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. *Applied Sciences*, *12*(2), 730. Retrieved from https://doi.org/10.3390/app12020730

Ghasemi, J., & Mahmoudi, N. (2024). The application of IoT devices in evidence collection and preservation in legal investigations in the common law legal system of Western countries. *Proceedings of the 2024 IST Conference*, 120–124. Retrieved from https://doi.org/10.1109/IST64061.2024.10843627

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312. Retrieved from https://doi.org/10.1109/COMST.2015.2388550

Grispos, G., Studiawan, H., & Alrabaee, S. (2024). Internet of Things (IoT) forensics and incident response: The good, the bad, and the unaddressed. *Forensic Science International:*

Digital Investigation, 48, Article 301671. Retrieved from https://doi.org/10.1016/j.fsidi.2023.301671

Islam, M., Mahin, M., Khatun, A., Debnath, B., & Kabir, S. (2019). Digital forensic investigation framework for Internet of Things (IoT): A comprehensive approach. *Proceedings of the 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 1–6. Retrieved from https://doi.org/10.1109/ICASERT.2019.8934707

Islam, M., Mahin, M., Khatun, A., Roy, S., Kabir, S. & Debnath, B. (2019). A comprehensive data security and forensic investigation framework for cloud-IoT ecosystem.

Kandwal, N. (2024). Experiencing IoT forensics in 2024: Navigating the latest trends. Retrieved from https://karnavatiuniversity.edu.in/experiencing-iot-forensics-in-2024-navigating-the-latest-trends/

Kaushik, K., Bhardwaj, A. & Dahiya, S. (2023). Smart home IoT forensics: Current status, challenges, and future directions. *Proceedings of the 2023 International Conference on Advances in Computing, Communication and Control Technology (InCACCT)*, 716–721. Retrieved from https://doi.org/10.1109/InCACCT57535.2023.10141730

Kumar, G., Saha, R., Lal, C. & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems, 120*, 433–450. Retrieved from https://doi.org/10.1016/j.future.2021.02.016

Mahmood, H., Arshad, M., Ahmed, I., Fatima, S. & Ur Rehman, H. (2024). Comparative study of IoT forensic frameworks. *Digital Investigation, 49*, 301748. Retrieved from https://doi.org/10.1016/j.fsidi.2024.301748

Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., & Rehman, H. U. (2024). Comparative study of IoT forensic frameworks. *Forensic Science International: Digital Investigation, 49*, Article 301748. Retrieved from https://doi.org/10.1016/j.fsidi.2024.301748

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges, and prospective measures. *Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 336–341.

Mahmud, H., Ragib, H. & Shams, Z. (2017). Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV). Retrieved from https://doi.org/10.1109/IEEE.ICIOT.2017.13

Mazhar, M. S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M. H., Rehman, A. U., Shafiq, M. & Hamam, H. (2022). Forensic analysis on Internet of Things (IoT) device using machine-to-machine (M2M) framework. *Electronics, 11*(7), 1126. Retrieved from https://doi.org/10.3390/electronics11071126

Mishra, N. & Pandya, S. (2021). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access, 9*, 59353–59377. Retrieved from https://doi.org/10.1109/ACCESS.2021.3073408

Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D. & Azer, M. A. (2023). IoT vulnerabilities and attacks: SILEX malware case study. *Symmetry, 15*(11), 1978. Retrieved from https://doi.org/10.3390/sym15111978

Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016). Internet of Things (IoT): Taxonomy of security attacks. *Proceedings of the 2016 3rd International Conference on Electronic Design (ICED)*, 321–326.

Nieto, A., Rios, R., & Lopez, J. (2017). A methodology for privacy-aware IoT-forensics. Retrieved from https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.293

Oriwoh, E., Jazani, D., Epiphaniou, G. & Sant, P. (2013). Internet of Things forensics: Challenges and approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. Retrieved from https://doi.org/10.4108/icst.collaboratecom.2013.254159

Perumal, S., Norwawi, N., & Raman, V. (2015). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. *Proceedings of the 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, 19–23.

Rudrakar, S., Rughani, P., & Sadineni, L. (2025). Digital forensics and incident response management model for IoT based agriculture. *Scientific reports*, *15*(1), 17797. Retrieved from https://doi.org/10.1038/s41598-025-02635-2

Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation, 28*, S22–S29. Retrieved from https://doi.org/10.1016/j.diin.2019.01.012

Sharma, S., Malik, A. & Sharma, A. (2023). A survey on blockchain based IoT forensic evidence. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/377634112_A_survey_on_blockchain_based_IoT_forensic_evidence

Silva, T. J., Oliveira Jr., E., Pereira, M. E., & Zorzo, A. F. (2025). A review study of digital forensics in IoT: Process models, phases, architectures, and ontologies. *Forensic Science International: Digital Investigation, 53*, Article 301912.

Sivanathan, A. (2020). *IoT behavioral monitoring via network traffic analysis* [Preprint]. ArXiv. Retrieved from https://arxiv.org/abs/2001.10632

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 163–167.

Weber, R. H. (2010). Internet of Things — New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. Retrieved from https://doi.org/10.1016/j.clsr.2009.11.008

Yaqoob, I., Hashem, I. A. T., Ahmed, A. & Kazmi, S.M.A. (2019). Choong Seon Hong, Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Retrieved from https://doi.org/10.1016/j.future.2018.09.058.