WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

IoT Device Exploitation and Security Breaches

Aditya Patil

LL.M. Student, **Deccan Education Society's Shri. Navalmal Firodia Law College, Pune**

ABSTRACT

Opening Line The rapid growth of the Internet of Things (IoT) has connected everyday devices such as smart phones, cameras, watches, home appliances and vehicles to the internet. While these devices provide convenience and automation, their continuous collection and exchange of data also creates opportunities for cybercriminals to exploit security weaknesses. Weak passwords, outdated software, insecure networks and poor security design can allow unauthorised persons to access IoT devices and misuse the information stored or transmitted through them.

Legal Background In India, unauthorised access to computer systems and misuse of electronic information are addressed primarily under the Information Technology Act, 2000. Provisions relating to unauthorised access, data theft, identity-related offences and other forms of computer-related misuse may become relevant when IoT devices are compromised. However, the rapid development of connected technologies creates challenges in applying existing criminal law to new forms of technological exploitation.

Present Status The increasing use of smart devices in homes, workplaces, healthcare and transportation has expanded the possible impact of security breaches. A compromised IoT device may be used to obtain personal information, monitor individuals, interfere with connected systems or become part of a larger cyberattack. Lack of regular security updates and limited awareness among users further increase these risks.

Technology Perspective IoT security requires protection at the device, network and data levels. Strong authentication, regular software updates, encryption, secure device design and user awareness can reduce vulnerabilities. Cooperation between manufacturers, service providers, users and law-enforcement agencies is also necessary for effective prevention and investigation of IoT-related offences.

Research Problem The existing legal framework raises questions about whether present criminal laws are sufficiently equipped to address the unique nature of IoT exploitation, particularly issues of attribution, privacy, evidence collection and responsibility of device manufacturers.

Hypothesis A combination of stronger cybersecurity standards, clearer legal responsibilities and effective law-enforcement mechanisms may improve the prevention and investigation of IoT-related security breaches.

Aims and Objectives To examine the nature of IoT device exploitation and security breaches. To study the existing Indian legal framework relating to IoT-related cyber offences. To identify major security and investigative challenges. To examine issues of privacy, digital evidence and criminal responsibility. To suggest measures for strengthening IoT security and legal responses.

Keywords: Internet of Things, IoT Security, Cybercrime, Security Breaches, Information Technology Act, Privacy, Digital Evidence, Cybersecurity, Criminal Law, Technology.

1. INTRODUCTION

Technology is no longer limited to computers and mobile phones. Everyday objects are increasingly being designed with sensors, software, communication capabilities and internet connectivity. A person may use a smart watch to monitor health information, a smart camera to observe a house, a connected vehicle to obtain navigation and diagnostic information, or a smart appliance that can be controlled through a mobile application. These devices form part of what is commonly referred to as the **Internet of Things (IoT)**. The significance of IoT lies not merely in the fact that devices are connected to the internet. Its important feature is the interaction between the digital environment and the physical world. IoT devices can sense their surroundings, collect information, communicate that information to another system and, in many situations, perform an action on the basis of processed information. NIST describes IoT devices as devices having at least one sensor or actuator for interaction with the physical world and at least one network interface for interaction with the digital world.[1]

[1] National Institute of Standards and Technology (NIST), *IoT Device – Glossary*

This development has considerable benefits. Connected systems can improve healthcare, transportation, home security, industrial production and public services. At the same time, the same connectivity creates vulnerabilities. If a smart camera is compromised, for example, the attacker may obtain access to private recordings. If a connected vehicle or industrial control system is manipulated, the consequences may extend beyond loss of data and may affect physical safety. The criminal law implications of IoT therefore require attention. Traditional cybercrime generally focuses upon unauthorised access to computers, data theft, identity theft or online fraud. IoT-related offences can involve these activities, but they may additionally involve manipulation of physical devices and cyber-physical systems. The legal question is consequently not limited to whether an offender accessed a computer without permission. It may also involve what the offender did through the compromised device, what harm resulted, who can legally be held responsible and how the electronic evidence can be proved before a court.

The Indian legal system has developed significantly in response to technological changes. The Information Technology Act, 2000 remains an important legislation dealing with computer-related offences and electronic transactions. The Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 have subsequently replaced the earlier criminal law framework and introduced provisions that are relevant to investigation and proof of electronic material. The central concern of this paper is therefore whether the existing Indian legal framework can effectively address the distinctive problems created by IoT exploitation and security breaches.

2. UNDERSTANDING THE INTERNET OF THINGS

2.1 Meaning and Concept of IoT

There is no single universally accepted definition of the Internet of Things. This is partly because IoT is not one particular technology or device. It represents an environment in which different physical objects, sensors, software systems, networks and users interact with one another. NIST explains IoT in terms of networked components that can interact with the physical world through sensors and actuators.[2] In ordinary terms, an IoT device is a physical object which has some form of computing capability and is capable of communicating with other systems. The device may collect information through sensors, process that information and communicate it through Wi-Fi, Bluetooth, mobile networks or other communication technologies. Some devices also have actuators which allow them to perform an action in the physical environment.

For example, a smart door lock does not merely store information. It may receive an instruction from a mobile application and physically lock or unlock a door. A smart thermostat can collect temperature information and automatically control heating or cooling. A medical monitoring device can collect physiological information and communicate it to healthcare professionals or a cloud platform. Thus, IoT is better understood as an **ecosystem** rather than as a single device. A typical IoT system may contain the physical device, a mobile application, a communication network, cloud infrastructure and a user account. NIST similarly recognises that an IoT product may include the device together with companion applications, gateways and backend services.[3]

This interconnected structure is important from a criminal law perspective because a security weakness in one part of the system may affect another part. An attacker may not directly attack the device itself. Instead, the attacker may compromise the mobile application, steal a user's credentials or exploit the cloud service connected with the device.

2.2 Main Components of an IoT System

An IoT environment generally consists of four interconnected elements.

First, sensors and actuators interact with the physical environment. Sensors collect information such as temperature, movement, location, sound or biometric information. Actuators perform actions based upon instructions received from the system.

Second, communication networks provide the means through which information moves between the device and other systems. These may include Wi-Fi, Bluetooth, cellular networks or other communication protocols.

Third, software and applications allow users and systems to interact with the device. A mobile application may allow a person to operate a camera, lock a door or examine information collected by a wearable device.

Fourth, cloud or backend infrastructure may store, analyse or process information received from connected devices. Consequently, the security of an IoT system depends upon more than the physical security of the device itself.

The combination of these elements makes IoT useful but also creates multiple points at which an attacker may attempt to enter the system.

3. IOT DEVICE EXPLOITATION

IoT device exploitation refers to the misuse of weaknesses in an interconnected device or its supporting ecosystem to obtain unauthorised access, information or control. Exploitation may occur because of poor security design, weak authentication, outdated software, insecure communication or inadequate protection of data. The important feature of IoT exploitation is that the device itself may not appear to be a traditional computer. A camera,

[2] NIST, *Internet of Things – Glossary*
[3] NIST, *Cybersecurity for IoT Program*

vehicle, smart speaker or medical device may nevertheless contain software, memory, processors and network interfaces. From a security perspective, therefore, the device may become a target in much the same way as a conventional computer system.

3.1 Weak Authentication and Passwords

One of the common security weaknesses is inadequate authentication. Devices may be installed with weak passwords, reused passwords or poorly protected credentials. If an attacker obtains valid credentials, the attacker may be able to access the device without exploiting a complicated technical vulnerability. The problem becomes more serious where the same credentials are used across several services. A stolen password obtained from one source may consequently provide access to a connected camera, mobile application or cloud account.

3.2 Outdated Software and Firmware

IoT devices frequently remain in use for several years. During that period, vulnerabilities may be discovered in the software or firmware installed on the device. If the manufacturer does not provide security updates or the user does not install available updates, the vulnerability may remain exploitable. This raises an important question concerning responsibility. A consumer may reasonably assume that a device is secure when purchased. However, cybersecurity is not a one-time condition. The security of a connected product may depend upon continuing maintenance, updates and monitoring.

3.3 Insecure Communication

Information transmitted between an IoT device, mobile application and cloud server may contain personal or sensitive information. If communication is not adequately protected, an attacker may attempt to intercept, modify or redirect the information. The consequences may vary depending upon the nature of the device. In a fitness device, the information may relate to a person's activities and location. In a home camera, it may include video recordings from inside a private residence. In an industrial environment, it may concern operational information or production systems.

3.4 Malware and Botnets

Compromised IoT devices can also be used as part of larger cyber-attacks. An attacker may infect several connected devices and use them collectively for malicious activities. The owner of the device may not even know that the device has been compromised. This creates a special difficulty in criminal investigation. A device located in a victim's home may appear to be the source of malicious network traffic even though the actual offender is located elsewhere. Technical evidence is therefore necessary to distinguish between ownership of a device and control of that device at the relevant time.

4. SECURITY BREACHES AND THEIR CONSEQUENCES

An IoT security breach may involve unauthorised access, disclosure, modification, destruction or misuse of information or control of a connected device. The consequences depend upon the type of system involved.

4.1 Privacy Violations

IoT devices can collect information continuously and sometimes without the user actively interacting with the device. Cameras, microphones, location systems and health-related devices may therefore create detailed information about an individual's activities. A compromised device may consequently become a means of surveillance. The privacy concern is particularly serious when the device is located inside a home or is worn by an individual.

4.2 Financial Loss

IoT systems may also be connected with payment systems, subscriptions, online accounts or business infrastructure. Unauthorised access can therefore result in financial loss. An attacker may use stolen credentials, manipulate connected systems or obtain information which can subsequently be used for fraud.

4.3 Identity Theft and Impersonation

Connected devices may process usernames, passwords, account information and other identifying information. Where such information is stolen, it may be used for impersonation or fraudulent activities. The Information Technology Act, 2000 specifically addresses identity theft under Section 66C and cheating by personation through a computer resource under Section 66D.[4]

[4] The Information Technology Act, 2000, ss. 66C and 66D. Section 66C

4.4 Physical Consequences

One of the distinctive characteristics of IoT crime is the possibility of physical consequences. A cyber attack against an ordinary computer may primarily result in loss or alteration of digital information. In contrast, a compromised IoT system may affect a physical object. Manipulation of a connected lock, vehicle, industrial system or medical device could potentially have consequences in the physical world. This connection between cyber activity and physical harm makes IoT particularly significant for criminal law.

5. INDIAN LEGAL FRAMEWORK

5.1 Information Technology Act, 2000

The Information Technology Act, 2000 remains the principal Indian legislation dealing specifically with information technology and several categories of cyber offences.

Section 43 deals with unauthorised acts relating to computer systems and computer resources. It covers conduct such as unauthorised access, downloading or copying data, introducing computer contaminants, damaging or disrupting computer systems and altering or deleting information.[5] In an IoT environment, the provision may become relevant where a person obtains unauthorised access to an IoT device or its connected computer resource and causes the type of damage contemplated by the provision.

Section 66 becomes relevant where the acts referred to in Section 43 are committed dishonestly or fraudulently. Therefore, depending upon the facts and evidence, unauthorised access to an IoT system may attract criminal consequences rather than merely civil liability.[6]

Section 66C deals with identity theft and Section 66D deals with cheating by personation through a computer resource. These provisions may become relevant where compromised IoT accounts or credentials are used to impersonate another person or obtain an unlawful advantage.[7]

Section 66E addresses violation of privacy in specified circumstances involving capture, publication or transmission of images of private areas without consent.[8]

The Act therefore provides several provisions which can potentially be applied to IoT-related misconduct. However, it was enacted at a time when the present scale of interconnected devices had not developed. The central difficulty is therefore not necessarily the complete absence of law, but whether existing provisions adequately address the more complex forms of cyber-physical exploitation.

6. LIMITATIONS OF THE EXISTING LEGAL FRAMEWORK

The first difficulty is **attribution**. An IoT device may be physically owned by one person but controlled remotely by another person. Merely proving that an unlawful communication originated from a particular device may not establish who actually operated it.

The second difficulty concerns the **multiple actors involved in an IoT ecosystem**. A single product may involve a manufacturer, software developer, cloud provider, telecommunications provider and user. When a security vulnerability is exploited, identifying the legally responsible person may become difficult.

The third difficulty concerns **jurisdiction**. IoT data may pass through servers located in different countries. The victim, device manufacturer, cloud provider and alleged offender may all be located in different jurisdictions. Obtaining evidence across borders can therefore delay investigation.

The fourth difficulty concerns **technical evidence**. IoT evidence may exist in several forms and at several locations. Investigators may need to examine the physical device, router logs, mobile applications, cloud accounts, authentication records, IP addresses and timestamps. Failure to preserve any one of these sources may weaken the evidentiary chain.

7. DATA PROTECTION AND IOT

The privacy dimension of IoT cannot be separated from data protection. Many IoT devices collect information which can identify or relate to individuals. This may include names, location information, behavioural patterns, photographs, audio recordings, health-related information and device identifiers.

The Digital Personal Data Protection Act, 2023 establishes a framework governing the processing of digital personal data. Section 8 places obligations upon a Data Fiduciary in relation to processing of personal data and requires responsibility for compliance with the Act and rules made under it. In an IoT environment, the concept of responsibility becomes particularly important because personal data may travel through several stages. A device may initially collect information, a mobile application may transmit it, and a cloud service may store or process it. Each stage presents a potential security risk. The law therefore needs to be understood not merely in terms of the device itself but in terms of the complete data-processing ecosystem.

[5] The Information Technology Act, 2000, s. 43.
[6] The Information Technology Act, 2000, s. 66.
[7] The Information Technology Act, 2000, ss. 66C–66D.
[8] The Information Technology Act, 2000, s. 66E

The Supreme Court's decision in **Justice K.S. Puttaswamy (Retd.) v. Union of India** recognised privacy as a constitutionally protected fundamental right under Part III of the Constitution.[9]The decision is important for IoT because pervasive connected devices may enable continuous collection of information about an individual's private life. At the same time, the data protection framework and criminal law serve different purposes. Data protection law primarily regulates processing of personal data and related obligations, whereas criminal law deals with prohibited conduct and punishment. An IoT security breach may therefore raise issues under more than one legal framework.

8. CYBERSECURITY AND THE ROLE OF CERT-IN

Cybersecurity prevention is an important part of controlling IoT-related crime. The Indian Computer Emergency Response Team (CERT-In) functions under Section 70B of the Information Technology Act and plays an important role in responding to cybersecurity incidents. The CERT-In Directions dated 28 April 2022 require specified entities to maintain logs of their ICT systems securely for a rolling period of 180 days and make them available to CERT-In in accordance with the Directions.[10] The Directions also contain requirements concerning reporting of specified cyber incidents and maintenance of information by certain service providers.

The relevance of log retention to IoT investigations is considerable. Logs may help investigators establish when a device communicated with a server, from which IP address the communication occurred, whether an account was accessed and whether unusual activity occurred before or after an incident.

However, logs alone cannot automatically identify the offender. An IP address may establish a connection or point of origin, but further evidence may be required to establish who controlled the relevant account or device. Therefore, log evidence should generally be examined together with authentication records, device information, account records and other forensic material.

9. ELECTRONIC EVIDENCE IN IOT-RELATED CRIMES

Electronic evidence is likely to be central to the prosecution of IoT-related offences. Unlike traditional physical evidence, electronic evidence can exist simultaneously in several locations.

For example, a smart camera may contain local storage, while the same recording may also be uploaded to a cloud server. A mobile application may contain account information, while the cloud system may maintain access logs. A router may contain records showing communication between the device and external servers. The **Bharatiya Sakshya Adhiniyam, 2023** now governs the admissibility of electronic records under the present evidence law framework. Section 63 specifically deals with the admissibility of electronic records and provides requirements concerning electronic or digital records and the accompanying certificate in applicable cases.[11]

The importance of authenticity cannot be overlooked. An electronic record should not be treated as reliable merely because it exists in digital form. The circumstances in which it was created, stored, extracted and presented may become relevant. The statutory schedule to Section 63 itself recognises technical particulars such as the source of the digital record and device identifiers and includes provision for recording hash values.[12] This is particularly relevant to IoT evidence because the integrity of extracted data may become a central issue at trial.

10. JUDICIAL APPROACH TO ELECTRONIC EVIDENCE

Although the current law is governed by the Bharatiya Sakshya Adhiniyam, 2023, earlier Supreme Court decisions concerning electronic evidence remain important for understanding the development of Indian evidentiary principles. In **Anvar P.V. v. P.K. Basheer**, the Supreme Court dealt with the admissibility of electronic records under the former Indian Evidence Act, 1872. The Court emphasised the statutory requirements governing secondary electronic evidence and held that the requirements of Section 65B had to be satisfied for admissibility in the circumstances covered by that provision.[13]

The decision was subsequently considered and clarified by the Supreme Court in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**, which reaffirmed the importance of the statutory certification requirement under the former Section 65B framework.[14]

This is particularly important in IoT cases because data may be automatically generated by devices without direct human intervention. Questions may arise regarding whether the device was functioning properly, whether the clock was accurate, whether the data was altered, whether the extraction process affected the original information and whether the device or server from which the record was obtained can be reliably identified.

---

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[10] Indian Computer Emergency Response Team (CERT-In), Directions under Section 70B of the Information Technology Act, 2000, dated 28 April 2022
[11] The Bharatiya Sakshya Adhiniyam, 2023, s. 63
[12] The Bharatiya Sakshya Adhiniyam, 2023, Schedule to s. 63(4)(c)
[13] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[14] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

11. INVESTIGATION OF IOT-RELATED OFFENCES

Investigation of an IoT-related offence requires a broader approach than simply seizing the suspected device.

An investigating officer may need to identify:

1) The physical IoT device involved;
2) The manufacturer and model;
3) The device identifier;
4) The user account connected with the device;
5) The mobile application associated with it;
6) The router or network through which it communicated;
7) Relevant IP addresses;
8) Cloud-service records;
9) Authentication and login records;
10) Relevant timestamps;
11) Firmware and software versions; and
12) Other connected devices involved in the incident.

The investigator must also preserve the integrity of the electronic material. If a device is improperly handled or data is altered during examination, questions may arise regarding its authenticity.

Section 105 of the BNSS requires the process of search and seizure to be recorded through audio-video electronic means, including preparation of the list of things seized.[15] This provision is relevant where electronic devices are seized during investigation. More importantly for IoT cases, **Section 193(3)** of the BNSS requires the police report to include the **sequence of custody in the case of an electronic device**.[16] This recognises the importance of documenting the movement and handling of electronic devices during investigation.

The requirement is significant because IoT evidence may pass from the scene to the investigating officer, forensic laboratory and eventually the court. Maintaining a clear record of custody assists in addressing allegations of alteration or tampering.

12. PROBLEM OF ATTRIBUTION

Attribution is one of the most difficult issues in IoT-related criminal investigations. Suppose a smart camera connected to a particular household is found to have transmitted malicious traffic. The fact that the camera belonged to a particular person does not automatically prove that the owner committed the offence. The device could have been compromised by a third party.

Similarly, if an attacker gains access to a smart home through stolen credentials, the relevant digital activity may appear to originate from the victim's account. Without additional evidence, identifying the actual offender may be difficult. Therefore, attribution requires correlation of several forms of evidence. These may include device logs, IP addresses, login information, authentication records, timestamps, network traffic, cloud records, forensic examination and evidence relating to control of the relevant account.

13. PRIVACY CONCERNS ARISING FROM IOT

IoT technology creates a distinctive privacy problem because connected devices may operate continuously in the background. A smartphone generally requires some interaction before an application collects information, whereas a smart camera, wearable device or home assistant may continuously collect information as part of its ordinary operation. The information collected may reveal patterns of behaviour. For example, location information may reveal where a person lives or works. A smart home system may reveal when occupants are present. A health-related device may reveal information about an individual's physical condition or routine.

The privacy concern therefore extends beyond the unauthorised disclosure of a single piece of information. The combination of different data points may create a detailed picture of a person's life. The constitutional recognition of privacy in **Puttaswamy** provides an important framework for understanding

[15] The Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105
[16] The Bharatiya Nagarik Suraksha Sanhita, 2023, s. 193(3)(i)

these concerns.^18 In the context of IoT, privacy protection requires attention not only to the collection of data but also to its storage, sharing, security and subsequent use.

14. RESPONSIBILITY OF MANUFACTURERS AND SERVICE PROVIDERS

One of the unresolved issues in IoT security is the responsibility of manufacturers and service providers. A consumer usually purchases an IoT product primarily for its functionality. The consumer may not have the technical knowledge necessary to understand whether the device uses secure authentication, receives security updates or properly protects data.

This raises a broader question: to what extent should responsibility for cybersecurity be placed upon the consumer and to what extent should manufacturers and service providers be expected to adopt security measures at the design stage? A secure-by-design approach is particularly relevant. Security should not be treated merely as a feature that is added after a product has been developed. Manufacturers can consider secure authentication, encryption, software updates, vulnerability management, access controls and mechanisms for responding to security incidents during the development of the product. The issue becomes particularly important where the device is likely to remain in use for several years. A manufacturer that stops providing security updates shortly after sale may leave consumers exposed even though the product remains operational.

The question of legal responsibility, however, must depend upon the applicable statutory provisions, contractual arrangements, the nature of the vulnerability and the facts establishing knowledge, conduct and causation. A security vulnerability by itself should not automatically be treated as proof of criminal liability.

15. MAJOR CHALLENGES IN CONTROLLING IOT CRIMES

15.1 Rapid Technological Development

Technology develops faster than legislation. New devices and communication methods may become common before specific legal questions concerning them have been tested before courts.

15.2 Lack of Technical Awareness

Users may not understand basic security practices such as changing default passwords, installing updates or restricting unnecessary access.

15.3 Fragmented Responsibility

An IoT ecosystem may involve several independent entities. Determining which entity controlled a particular aspect of security may be difficult.

15.4 Cross-Border Nature of Cybercrime

IoT data can pass through foreign servers and international networks. Evidence may therefore be located outside the jurisdiction in which the offence is investigated.

15.5 Preservation of Evidence

Electronic evidence can be altered, overwritten or deleted. Delay in obtaining logs or cloud records may therefore make investigation more difficult.

15.6 Difficulty in Establishing Causation

In cases involving physical consequences, investigators may have to establish a connection between the digital interference and the physical result. This requires both legal and technical evidence.

16. PREVENTIVE MEASURES

Prevention should form an important part of the legal response to IoT-related crime.

1) Manufacturers should adopt **security-by-design principles**. Devices should not be released with easily guessable default credentials or unnecessary open services.
2) Manufacturers should provide **regular security updates** for a reasonable period corresponding to the expected life of the product.
3) Users should be encouraged to use **strong authentication**, unique passwords and multi-factor authentication wherever available.

4) Sensitive information transmitted by IoT devices should be protected through **appropriate encryption and secure communication protocols**.

5) Organisations using large-scale IoT systems should maintain **logs and incident-response mechanisms** so that suspicious activity can be identified and investigated.

6) Law enforcement agencies require specialised training in **digital forensics and IoT architecture**. Traditional seizure of a physical device may not be sufficient when important evidence exists on cloud servers or connected applications.

7) Manufacturers, service providers, CERT-In and law enforcement agencies should cooperate in responding to vulnerabilities and preserving evidence.

19. SUGGESTIONS

The following measures may strengthen the Indian response to IoT-related crimes:

1) Security-by-design should be encouraged in the development of IoT products.

2) Manufacturers should provide reasonable security updates throughout the expected operational life of a device.

3) Minimum cybersecurity standards should be developed for categories of IoT devices having significant privacy or safety implications.

4) Users should receive clear security information at the time of purchase and installation.

5) Law enforcement agencies should receive specialised IoT forensic training.

6) Digital evidence protocols should be consistently followed during seizure, extraction, preservation and presentation of IoT evidence.

7) Manufacturers and service providers should maintain appropriate incident-response mechanisms and cooperate with lawful investigations.

8) International cooperation should be strengthened for obtaining cloud and cross-border electronic evidence.

9) Privacy safeguards should accompany IoT development, particularly where devices continuously collect personal information.

10) Legal and technological developments should be reviewed periodically, because IoT technology changes rapidly and new forms of exploitation may emerge.

20. CONCLUSION

The Internet of Things represents an important stage in the development of technology because it connects the digital world with everyday physical objects. Its applications extend from ordinary household appliances to healthcare, transport, manufacturing and other areas having significant social and economic importance. The same connectivity that makes IoT useful also creates security vulnerabilities. A compromised device can become a means of unauthorised surveillance, data theft, identity misuse, fraud or manipulation of physical systems. IoT-related crime therefore presents challenges that are not always adequately explained by traditional categories of cybercrime. Indian law already provides a foundation for addressing several forms of such misconduct. The Information Technology Act, 2000 remains central to computer-related offences. The Digital Personal Data Protection Act, 2023 is relevant to the processing and protection of personal data. The Bharatiya Sakshya Adhiniyam, 2023 provides the current framework for electronic evidence, while the Bharatiya Nagarik Suraksha Sanhita, 2023 contains provisions relevant to electronic investigation, search and seizure and the sequence of custody of electronic devices.

However, legal provisions alone cannot provide complete protection. IoT security is dependent upon the conduct of manufacturers, software developers, service providers, users, investigators and other stakeholders. Effective investigation also requires technical expertise and careful preservation of digital evidence. The central challenge for criminal law is therefore to respond to technological misuse without treating every technical failure as a criminal offence. A distinction must be maintained between accidental vulnerability, inadequate security, civil or regulatory responsibility and deliberate criminal exploitation. At the same time, where intentional exploitation causes harm, the law must be capable of identifying the offender and proving the connection between the offender, the compromised device and the resulting conduct.

The future of IoT will depend not only upon greater connectivity but also upon greater trust and security. A balanced legal approach should therefore combine criminal accountability with preventive cybersecurity, privacy protection, responsible technology design and effective digital investigation.

21. Bibliography

Statutes

1. The Information Technology Act, 2000.
2. The Digital Personal Data Protection Act, 2023.

3. The Bharatiya Nyaya Sanhita, 2023.
4. The Bharatiya Nagarik Suraksha Sanhita, 2023.
5. The Bharatiya Sakshya Adhiniyam, 2023.

Cases

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
3. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
4. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

Reports and Other Materials

1. National Institute of Standards and Technology (NIST), *Internet of Things (IoT) Cybersecurity Publications and Guidance*.
2. NIST, *Networks of 'Things'*, Special Publication 800-183.
3. NIST, *Internet of Things (IoT) Component Capability Model for Research Testbed*, NISTIR 8316.
4. Indian Computer Emergency Response Team (CERT-In), *Directions under Section 70B of the Information Technology Act, 2000*, 28 April 2022.
5. Ministry of Electronics and Information Technology, Government of India, materials concerning cybersecurity and IoT.