IoT Forensics with emphasis on Radar Technology

Syed Fazal Mehdi Moosvi
Student, SoS Digital Forensics, Malla Reddy University, Hyderabad, India
fazalmoosvi46@gmail.com

Abstract

Radar enabled IoT devices are becoming common in homes, vehicles, and public areas, creating a new form of forensic evidence: continuous, unintentionally generated RF patterns that reveal presence, movement, and even physiological signals. This paper proposes a radar focused IoT forensics approach that explains how investigators can locate relevant sensors, acquire their data, and understand the RF traces they generate.

The document outlines how chirps, micro Doppler phenomena, and MIMO arrays empower mm Wave and UWB sensors to detect intricate human patterns such as walking, movements, and respiration[2]. It evaluates significant radar systems, including Google Soli, automotive ADAS radars, Wi-Fi CSI based sensing, and industrial mm Wave units, while addressing challenges such as proprietary data formats, limited local storage capacity, and dependence on cloud based services[4][5][10].

The paper presents a range of forensic approaches for analysing radar data, including I/Q signal capture, point cloud examination, and activity based analysis, alongside cross validation with additional sensors[36]. It discusses methods such as spectrogram inspection, reconstruction of gait and gestures, and deep learning–based activity recognition, as well as data fusion with optical and Wi-Fi sources. The study also considers anti forensic challenges like jamming and spoofing, highlighting potential signs of manipulation, including abnormal motion patterns and atypical spectral characteristics[11][32].

The paper concludes by evaluating how radar derived evidence aligns with IEA and BSB legal standards and how investigators can adopt it responsibly, in a manner comparable to data from wearable devices or vehicle event data recorders. As environments become increasingly “radiologically active,” radar sensors are positioned to function as unobtrusive witnesses, providing a robust scientific and practical foundation for contemporary digital forensics.

Keywords: IoT Forensics, Radar Technology, mm Wave, Ultrawideband, Micro Doppler, Digital Evidence, Bharatiya Sakshya Adhiniyam.

1 Introduction

The integration of the IoT gadgets and advanced RF (radio frequency) sensing technologies is redefining the digital evidence nature of current investigations. Conventional digital forensics has concentrated on intentional user actions like access to

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_16

files or writing of messages. Unlike this, smart environments can now be used to continuously and passively gather data, converting human presence, movement, and physical condition into data that can be seen even in the absence of direct interaction with devices[3][28]. The IoT systems that are central to this shift are created through radar in the millimetre wave (mm Wave) and ultrawideband (UWB) spectra. These sensors, installed in gadgets such as smart homes and cars and mobile phones among others, produce high quality electromagnetic models of physical activity. Together, they create a continuing digital shadow of human behaviour that increases the possibilities and capabilities of modern digital forensic analysis[4][11][16].

The research paper is a proposal of a single forensic framework named as A Comprehensive Forensic Analysis of Radar Based IoT Sensors in Smart Environments. The framework is driven by the unique characteristics of radar data which is based fundamentally on discrete, logic based artifacts of a traditional computing system. Radar evidence is continuous, probabilistic in nature and is based on physical phenomena. It records fine grained micro Doppler signatures like motion of the limbs, chest movement of the respiratory system during the sleeping period or the route taken by the vehicle in the milliseconds before hitting the other vehicle. With the growth of radar enabled sensors being more ubiquitous, they act as a silent observer, able to confirm alibis, and rebuild crime scenes with their temporal and spatial accuracy what once needed high security surveillance systems.

The forensic worthiness of radar sensing is also supported by the fact that radar sensing is resilient where optical sensors fail. Radar has the benefit of working in the dark, smokes, and non-metallic covering; it provides the investigators with a powerful sensory modality that is resistant to concealment by the environment. But there is serious technical difficulty in extraction and interpretation of radar data. Radar data unlike normal standardized digital items in persistent media are usually volatile and are held in volatile circular buffers or processed at the edge to proprietary feature representation after which they are disposed of. Lack of standardized forensic equipment to acquire raw In Phase/Quadrature (I/Q) signals and interpret point clouds places a large capability gap in investigative agencies[36].

What adds to these problems is the fact that there is a very dynamic legal system which deals with the admissibility of complicated electronic evidence. The Indian Evidence Act, 1872 is replaced by the Bharatiya Sakshya Adhiniyam, 2023 in India and in this process, courts reevaluate the manner of evaluating digital records. Under the BSA, electronic data can be considered primary evidence in case the integrity and chain of custody is strictly proven. The similarities and differences between the radar artifacts that are usually produced without any human intervention and the certification provisions of Section 63 of the BSA in comparison between that and the previous Section 65B of the IEA are critically analysed in this paper.

This study aims at operationalizing radar forensics by incorporating signal processing theory, device specific forensic techniques, and modern legal jurisprudence. Going beyond what is theoretically possible, it describes the practical ways of determining the

radar sensors at a crime scene, obtaining volatile data, and using deep learning models to recreate human activities[3]. With the emerging technologies of IoT based passive sensors shifting into active monitors of physical reality, the community of forensic professionals should be ready to decipher the ever-increasing RF signatures that are ubiquitous in the contemporary world.

2 Physics of Radar Sensing in Forensics

To derive probative value of radar based IoT devices, the forensic examiner has to have an insightful knowledge of the physics involved. Radar systems transmit electromagnetic waves and analyse their reflections to measure the distance, velocity and angle unlike cameras, which record the photons to create 2D images. The interactions of these waves with the human body produce certain signal artifacts that can be reconstructed in a forensic way to determine the action or a person[3][28].

2.1 Frequency Modulated Continuous Wave (FMCW)

The prevailing architecture used in contemporary commercial radar systems especially within automotive and industrial domains is Frequency Modulated Continuous Wave (FMCW) radar[22]. As a result of its high spatial resolution and its capacity to evaluate both target range and velocity simultaneously, FMCW radar has largely ousted pulsed radar in shortrange sensing utilizations[34].

2.1.1 The Chirp Signal and Range Resolution

In an FMCW radar, a frequency modulated chirp is emitted by the transmitter whose signal frequency is linearly varied with the time[27]. When a target is hit, the reflection signal has a small time difference with respect to the sent signal. The radar uses the received and transmitted signal to give a comparison on the intermediate or beat frequency that then coded the range of the target. This is accomplished by means of a mixer to mix the outgoing and incoming signal to generate an Intermediate Frequency (IF) signal. The beat frequency (f b) is directly proportional to the distance of the target (R), and this phenomenon is determined by the slope of frequency chirp (S) where (c) is the speed of light[27].

$$fb = S \cdot \frac{2R}{c}$$

In the case of investigations, range resolution is also an important measure that describes the range in which the radar is able to distinguish two neighbouring objects. ($\boldsymbol{d}$res), which determines how well the system is able to differentiate between two close individuals or objects in a room or a person standing near a wall. The range resolution is proportional to the inverse of bandwidth (B) of the chirp:

$$dres = \frac{c}{2B}$$

Recent IoT sensors, e.g., in 60 GHz or 77 GHz bands, can make use of 4 GHz bandwidth. This gives a theoretical range of the range of 3.75 cm. At this high granularity value, forensic data obtained by an FMCW sensor can clear a scene to the fine structural features distinguishing between limbs or discerning between a victim and an aggressor in an altercation[27].

2.1.2 Velocity Estimation and the Doppler Effect

In addition to range estimation, FMCW radar uses target velocity based on the phase difference between consecutive chirps. Even extremely small motions between transmissions of a target introduce phase shifts in the received signal. The corresponding phase rotation frequency (f d) is the frequency of the Doppler shift, which allows calculation of the radial velocity of the target (v), with lambda denoting the wavelength of the signal[22].

$$v = \frac{\lambda . fd}{2}$$

This capability is particularly significant for forensic reconstruction, such as determining vehicle speed from an event data recorder or estimating the velocity of a hand gesture captured by a smart hub. Because it is based on direct physical measurements of motion, Doppler derived velocity evidence is inherently difficult to falsify without advanced electronic warfare techniques[15].

2.2 Ultrawideband (UWB) Impulse Radar

Whereas FMCW radar operates in the millimetre wave band, Ultrawideband (UWB) technology has secured a niche in the secure access control and high accuracy localization applications, primarily through the IEEE 802.15.4z standard[22]. UWB radar systems work by the transmission of very short duration pulses of generally a few nanoseconds or few picoseconds in the very wide spectrum of frequency bandwidth of over 500 MHz[1][2].

UWB has great forensic benefits compared to narrow band radio technologies. The ultrashort pulses combined with a wide bandwidth allow very precise time of flight measurements, and with centimetre level accuracy position can be determined, and multipath interference, which typically causes the localization of RSSI based Wi-Fi to be invalid, is significantly reduced[1][33][34].

Also, as an enhancement of the human respiration-induced changes in the Channel Impulse Response (CIR), UWB radar is used to detect the presence[3]. The stored CIR data can thus be examined in a way that forensic study can be considered a kind of life detecting in that even when the subject was motionless and silent, the investigator can be able to determine that a living person had occupied a space at that particular time[1][2][34].

2.3 The Micro Doppler Effect: A Biometric Fingerprint

One concept in radar based forensics is the micro Doppler effect. In addition to the velocity of the

body as a whole, small motions of arms, legs and even the torso bring about additional frequency variations in the radar echo resulting in characteristic micro Doppler patterns. Mathematically, when the amplitude of a vibrating or rotating part (such as a swinging arm) has a range R(t) the received signal amplitude can be modified by modulation as:

$$\phi(t) = \frac{4\pi R(t)}{\lambda}$$

The time derivative of the signal phase obtains the instantaneous change in frequency which is also known as the micro Doppler frequency. Since human gait features (limb length, swing cadence, asymmetry of movement) are determined by physiological factors of an individual, the micro Doppler patterns that are formed may serve as the behavioural biometrics. Forensic gait analysis by radar therefore can identify individual members of a group of people, or tell the difference between a human and an animal, only using RF spectrograms of the patterns obtained by a sensor that has been hacked in to[32].

Similarly, periodic movement of the chest wall as the diaphragm moves during the breathing process is generally observed to produce minor phase modulations in the radar reflection with magnitude of order 1 -12 mm and even smaller amplitude fluctuations connected with cardiac activity. Forensic analysts can determine physiological conditions by deriving this set of vital signs signatures using unprocessed radar data, e.g., higher heart rates indicate stressful states, or lack of respiratory activity indicates a stoppage of breathing[11].

2.4 MIMO and Spatial Reconstruction

The modern radar systems are increasingly using Multiple Input Multiple Output (MIMO) antenna arrays in estimating Angle of Arrival (AOA) of reflected signals. The radar is able to estimate the azimuth and the elevation of an object by examining the phase difference in several receive antenna elements. The addition of this spatial information converts one dimensional range data or two dimensional range-Doppler representations to three dimensional point clouds with added velocity information (x, y, z, v). Within the forensic context, MIMO obtained point clouds allow an investigator to determine the movement of subjects in a physical space, with time. This ability is similar to a low resolution, privacy preserving version of LiDAR, enabling movement tracks within the buildings or vehicle paths on roads to be generated. These types of geometric reconstructions can be associated with floor plans or crime scene plans, to give a spatially located explanation of events.

3 Survey of Major Radar Platforms

Closeness to the various hardware ecosystems that are being rolled out is needed to implement radar forensics constructively. The resultant evidence differs significantly in terms of format, resolution, and accessibility that are contingent on platform.

3.1 Google Soli and Consumer Electronics

Google's Project Soli represents the miniaturization of radar for consumer interfaces. Using a 60 GHz mm Wave sensor, Soli was integrated into the Pixel 4 smartphone and the Nest Hub (2nd Gen)[7][8].

- Project Soli by Google is a form of miniaturization of radar, used to bring it to consumer interfaces. Soli was designed using a 60 GHz mm Wave sensor and implanted into the Pixel 4 smartphone and Nest Hub (2nd Gen)[4][16].
- **Forensic Artifacts:** Google Soli is based on fast chirp FMCW radar to identify fined grained hand gestures. Instead of the raw radar signal samples being stored, Soli allowed devices to store higher level derived outputs, e.g. the detected gesture events or measurement of sleep. Such ready-made records may subsequently provide as useful forensic artifacts, with the reference to user interaction or physiological presence at particular moments in time[7][8][28].
- **Deep Soli Dataset:** A dataset of research built using Google Soli, including Deep Soli, has been published in HDF5 format holding Range-Doppler maps. The datasets allow forensic researchers to train machine learning classifiers that are capable of reconstructing particular hand interactions using recovered radar sensor buffers that may prove that a suspect was actively engaging with a device at a specific time[6][7].
- **Object Recognition (Radar Cat**): Radar systems have been demonstrated to identify objects by their radar cross section and scattering properties in addition to gesture recognition (radar cat). Forensically, this implies that a Soli-enabled device might capture the nature of object in front of it that would enable it to differentiate between objects like a hand, a mobile phone, or a weapon[8].

3.2 Automotive ADAS and EDR Systems

The automotive industry has been the most accepting of mm Wave radar, mostly operating at 77 GHz, to provide Advanced Driver Assistance Systems (ADAS)[4][9][10].

- **EDR**: The current Event Data Recorders (EDRs) represent the black boxes of vehicles. Although the parameters measured by the older versions of EDR were mostly limited to vehicle speed and braking force, the newest versions of EDR are dependent on Controller Area Network (CAN) bus which enables the storage of object lists generated by onboard radar processors[9]. These lists of objects record the relative location, velocity and approximate dimension of the identified obstacles such as other vehicles and pedestrians in the critical seconds before a collision, a situation which offers investigators a comprehensive shot of the situation before the impact event[10].

- **Tesla Autopilot Telemetry:** Tesla vehicles can be characterized by the scope and detail of data that can be logged on-board. The car computer systems store rich telemetry of the Autopilot sensor package which historically includes forward facing radar but more recent

models are more dependent on vision based systems[14]. This type of data may be acquired in a forensic manner, which may require proprietary interfaces, special cables, or high system (root) access to provide comprehensive snapshot of the nearby traffic environment in point cloud form[14]. These reconstructions allow the investigator to recreate the pre incident scenes with fidelity, which allows statements by the drivers of the availability or behaviour of other vehicles to be corroborated or refuted independently[14].

3.3 Wi-Fi CSI Sensing

Although not a special radar device, Wi-Fi Channel State Information (CSI) sensing recreates radar such as surveillance with standard Wi-Fi packets

- **Mechanism:** Wi-Fi signals travel in the environment by scattering around objects of the environment, as they pass through a transmitter (router) and a receiver (device). The multipath propagation is perturbed by human action, which effects the difference in the amplitude and phase of CSI between subcarriers[25][33].

- **Forensic Utility:** The Wi-Fi signals can permeate the walls and therefore CSI data can be utilized in through wall surveillance. The log of CSI historical logs (where this feature is activated in the case of network diagnostics or sensing) can be analysed in order to determine the individuals who are in a building, their approximate location, and their activity level[25]. Comparative analyses indicate that mm Wave radar is more resolute (average accuracy of activity recognition is approximately 32 times higher), whereas Wi-Fi sensing is widespread enough to become an important source of evidence in the conditions that do not have specific sensors[4][11][20].

3.4 Industrial and Smart Home Sensors

Examples of such companies include Texas Instruments (TI) and Infineon which supply the mm Wave chipsets (e.g. TI IWR6843, Infineon BGT60) used to power a host of industrial and smart-home devices, ranging through occupancy sensors in HVAC systems to fall detectors on the elderly[21].

- **Data Characteristics:** These devices are normally processing raw radar information at the edge, and exporting and compact terms of data, like point cloud or state occupation vectors over protocols like MQTT or WebSocket. Assuming that smart building infrastructures are involved, forensic investigators might come across radar sensors and see a detailed occupancy heatmap with a time stamp of room usage and approximate occupancy numbers.

4 Forensic Framework: Analysis of Radar Based Evidence

In order to methodically misuse these technologies, this paper is a suggested forensic framework

that is adapted to the specifics of RF sensing: Identification, Acquisition, Analysis, and Verification.

4.1 Identification of Radar Artifacts

The first step in any digital investigation is the identification of potential evidence sources. Radar sensors are often physically inconspicuous, hidden behind plastic casings or integrated into multisensory arrays.

identification of the possible sources of evidence is the initial procedure in any digital investigation. Radar sensors can be very small physically, being enclosed in plastic casing or embedded in multisensory arrays.

- **Visual and Digital Inspection:** physical examination of smart devices should be conducted by investigators to identify non-optical apertures or other regulatory markings to show that the device is operating at 60 GHz or 77 GHz, including FCC identifiers of 60 GHz and 77 GHz bands. Digitally, network reconnaissance software such as Nmap could be employed to identify devices that open ports that are linked to telemetry streaming, such as those used by mm Wave development software or proprietary UDP based data feeds[32].

- **Network Traffic Analysis:** Network traffic achieved through continuous sensing generates characteristic network traffic signature. Periodic bursts of high bandwidth and use of UDP packet capture such as Wireshark has the potential to reveal periodic bursts of high bandwidth packet capture. Periodic bursts of high bandwidth packet capture are usually linked to point cloud streaming or periodic MQTT heartbeat reports of sensor status. The identification of such patterns is able to establish the presence of dynamic radar sensing and recording in the interrelated environment. The data acquisition methodologies are as follows: The radar data procurement is marred with the vagaries of the information. Raw data undergoes processing and is dropped quickly; acquisition policies need to be directed towards data on the fly capture and prepared logs recovery.

4.2 Data Acquisition Methodologies

The information is volatile and this makes the acquisition of radar data difficult. Raw data is quickly used and throw away, therefore acquisition strategies should be aimed at capturing data in transit or retrieval ready logs.

4.2.1 Raw I/Q Data Capture

- **Raw I/Q data:** it is the richest format of evidence, and is not commonly stored on commercial equipment because it occupies a lot of space. Live Capture Live capture can be used in situations that require capturing the output of a prototype driver/hardware device, or that need access to the LVDS/CSI2 device the sensor is attached to. capture cards such as the (TI DCA1000EVM) can be used to access the sensor LVDS/CSI2 outputs.

This enables the diversion of the live radar stream to forensic workstation to store and analyse it[15][36].

- **Buffer Dumping:** In case of compromised IoT, an advanced method of either JTAG or UART interfacing the device can give the investigator the ability to dump the contents of the device RAM possibly containing the circular buffer of the latest I/Q samples before overwriting.

4.2.2 Point Cloud and Telemetry Extraction

More commonly, investigators will encounter processed data.

More often, investigators are going to be exposed to processed data. Cloud Acquisition: Smart home devices (e.g., sleep trackers) are connected to the cloud with the metrics they derive. Acquisition is a legal operation (warrants) that is aimed at acquiring JSON or CSV logs of events (e.g., "motion detected" or respiration rate) of the service provider (e.g., Google, Amazon).

- **Vehicle EDR Extraction:** In the case of automotive radar, the standard tools such as the Bosch CDR (Crash Data Retrieval) system are connected to the diagnostic port of the car to retrieve the EDR report. The data of the radar object list, which are stored in the non-volatile memory, in that the event that triggered the event (crash) occurred is in the form of a freezeframe in this report[24].

4.2.3 Wi-Fi CSI Extraction

CSI data generally needs a special firmware (e.g. Nexmon) on the Wi-Fi interface. Forensically, when a router has been captured, the investigators may search it to find out the debug logs or may place a passive monitoring software on the network to gather CSI packets that are being broadcasted by the router in the process of recreating the crime scene. In this section, techniques of analysis and interpretation will be discussed. After being obtained, the abstract numerical data should be converted into a forensic narrative.

4.3 Analysis and Interpretation Techniques

Once acquired, the abstract numerical data must be translated into a forensic narrative.

4.3.1 Spectrogram Analysis

The spectrogram (Time Velocity diagram) is the main instrument used in analysing motion. Through the use of Short Time Fourier Transform (STFT) the radar information, it is possible to have a visual representation of the Doppler history of the scene[13].

- **Activity Classification:** The spectrum signature of different human activities is different. The fall phenomenon is a sudden change in acceleration (high Doppler shift) and then an abrupt halting (zero Doppler) which involves a distinct L shape in the spectrogram[11].

When walking, it forms a sinusoidal envelope of the swinging extremities which forms a torso line. Such visual patterns enable forensic specialists to establish qualitatively the character of the recorded activity[13].

4.3.2 Deep Learning for Human Activity Recognition (HAR)

To quantify the analysis, Deep Learning models are employed.

- **Neural Networks:** Convolutional Neural Networks (CNNs) and Long Short term Memory (LSTM) networks trained on radar datasets can classify activities with high precision. For instance, feeding a range Doppler map into a trained CNN can classify an action as "punching," "kicking," or "walking" with accuracy rates often exceeding 90%[3].
- **Forensic Application:** Investigators can use pretrained models (verified against standard datasets like "Deep Soli") to automatically flag suspicious activities in large volumes of seized radar logs, creating a timeline of relevant events[6][7][13].

4.3.3 Gait Analysis and Identification

Advanced analysis of micro Doppler signatures enables gait recognition.

- **Biometric Identification:** The specific kinematics of a person's walk stride length, cadence, limb velocity are encoded in the micro Doppler envelope. Research indicates that radar based gait recognition can achieve identification accuracies of up to 97% in controlled environments. In a forensic point of view, this could potentially relate a suspect to a crime scene based solely on the radar logs of their movement, even if their face was unidentifiable[32].

4.4 Verification and Cross Checking

Radar evidence is strongest when combined with other sources of data.

- **Multimodal Fusion:** By matching radar timestamps with CCTV footage, smart lock access history, or wearable device data (heart rate, accelerator) a strong chain of evidence is formed[26]. When a radar sensor reads a fall at 10:42 PM, whilst the victim smartwatch registers a sudden increase in heart rate then nothing happening at the same second, the probability of the two independent events being a true event is greatest, which is in line with the principle of corroboration necessary in a court of law[26].

5 Legal Admissibility: The Bharatiya Sakshya Adhiniyam (2023)

Without a legal framework to admit radar evidence, the technical capability to harvest radar evidence will be irrelevant. In India, the Indian Evidence Act, Indian Evidence Act (IEA) 1872 has to be replaced with the Bharatiya Sakshya Adhiniyam, BSA 2023, this is a shift in how electronic evidences are treated[12].

5.1 From Section 65B (IEA) to Section 63 (BSA)

Electronic records came under the Indian Evidence Act, 1872, under Section 65B, a certification was mandatory to prove the authenticity of the electronic evidence that was considered secondary. This clause often created confusion on the judges, especially with regard to who could issue the certificate, and whether the parameter was consistent to all types of electronic records[12][17].

This approach is modernized in BSA 2023:

- Expanded Definition: Section 2(1)(d) of the BSA expressly refers to a document to include electronic and digital records such as server logs, locational evidence and emails. Radar logs are digital records of occurrences that are physical in nature and hence they can be classified under this definition.

- Primary Evidence Status: Section 57 and 61 of the BSA suggest that electronic records created through proper custody could be regarded as primary evidence (which is equivalent to originating documentation), eliminating the necessity to prove they are secondary copies, as long as their integrity is not also challenged[17].

5.2 The Section 63 Certificate for Automated Sensors

Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), a replacement of Section 65B of the Indian Evidence Act, still provides that certification is required to establish the admissibility of electronic records, but adds specific measures in the event of automated systems, e.g. IoT sensors. Practically, this means that it has to be certified by a responsible custodian and a qualified technical expert. Integrity protection (such as cryptographic hash values and other technical information) must also be recorded on the certificate, to prove that radar data files have not been changed[17][31].

- **Dual Certification:** Section 63(4) requires the signature of two parties to the certification of the electronic records, which are the person in charge of the device (e.g. the owner or administrator of the system) and an expert involved in technology. This is especially important to radar forensics. A layperson, like a homeowner cannot make credible testament to the technical integrity of complex products, such as micro Doppler logs. The signature of the expert should be used to authenticate those technical procedures (to ensure that there is proper operation of the radar sensor and that cryptographic hash values of the extracted data correlate with the initial records), as well as to ensure that the interpretation of the radar signals is based on the recognized principles of science[17][31].

Chain of Custody and Hashing- Bharatiya Sakshya Adhiniyam highly values data integrity. In line with its requirements, the certification should confirm the fact that the appropriate computer system or device was operational within the time frame, in question. To ensure this requirement, the forensic investigators should produce cryptographic hash values like SHA256 values of radar data files as soon as they have acquired the radar data files. Such

hash values should be clearly stated in the Section 63 certificate, and thus, indicate that the information shown in the court is a precise and undistorted copy of the information obtained by the radar sensor[31].

5.3 Automated Data Without Human Intervention

The major difference in the BSA is the analysis of data generated in the absence of a human factor. Radar sensors are independent. Section 63(2) places prerequisites towards admissibility, that is, on the regularity of use of the device as well as its proper functioning[18].

- **Implication**: The main forensic question in the case of radar data is not to prove authorship, as would be the case with communications such as emails, but to prove reliability of the system which made the data. Then the forensic report should indicate that the radar sensor is a homogeneous, precisely met instrument and that the data logging procedure that it pre programs to execute is also consistent and precise. Such a strategy complies with the computer output doctrine, according to which radar obtained records are considered objective machine generated evidence rather than statements of a human or hearsay.

6 Anti Forensics: Threats and Countermeasures

As radar forensics matures, criminals will inevitably employ ant forensic techniques to evade detection or manipulate evidence.

6.1 Jamming and Denial of Service

With the maturity of radar forensics, the criminals will always use ant forensic tools to avoid detection or compromise the evidence[19].

6.1.1 Jamming and Denial of Service.

Jamming consists of releasing power RF noise in the frequency of operation of the radar (e.g. 77 GHz) to flood the Low Noise Amplifier (LNA) in the receiver.

- **Forensic Indicator:** When a radar sensor is jamming the sensor does not normally stop recording instead it records an abnormally high noise floor. This appears in spectrogram analysis as a broadband and high amplitude curtain effect across all Doppler bins which effectively masks valid target reflections. The ability to detect this remarkable spectral profile helps an investigator to differentiate between calculated RF interference and a non-nonmagical sensor defect.

6.2 Spoofing and Ghost Targets

Another threat is more complex and is known as spoofing whereby an attacker sends in

counterfeited radar signals to form ghost targets.

- **Mechanism**: This attack model involves using a transponder or Digital Radio Frequency Memory (DRFM) system by an adversary in order to intercept transmitted chirp by a radar and add a controlled time delay in order to alter range, as well as a phase shift in order to spoof velocity, and subsequently retransmit the spoofed signal. Such manipulation could either cheat Advanced Driver Assistance Systems into thinking it has encountered an object that is not there, like a ghost pedestrian, or can make smart home radar sensors think that there is a person where no one is.
- **Forensic Detection:** Spoofed radar returns cannot often produce complex micro Doppler modulations of a real physical object. A fabricated human target could e.g. have nominal walking velocity, but have no typical rhythmic limb swing patterns in spectrogram analysis. Besides, the continuously resending signals cause phase perturbation or interruptions which may be detected by looking at phase coherence between two consecutive chirps. Availability of this aberration can be a strong signal of the signal alteration and it is significant in detecting the tampered radar data streams.

6.3 Replay Attacks

Replay attack an attacker captures the RF signature of an authentic user (e.g. gait of a legitimate resident) and re-uses this to get around a biometric lock or spoof a false confession.

- **Countermeasure**: In an attempt to make the transmitted chirps invisible to an attacker, sophisticated radar systems can encode subtle pseudorandom modulations, also known as watermarks, into the transmitted chirps. In case the received signal does not have the intended watermark or has an irregular or old time stamp, it is said to have been replayed. Raw radar signal forensic analysis can therefore reveal the lack of these authentication markers which is potent evidence of signal replay or modification[23].

7 Discussion: Practical Challenges

Despite the potential, significant hurdles remain.

- **Data Volatility:** IoT devices typically have limited onboard storage, and high bandwidth radar data is often retained only briefly in circular buffers before being overwritten. In the absence of immediate live acquisition or established forensic readiness measures such as automated event synchronization to cloud storage critical evidentiary data may be irretrievably lost within minutes.
- **Proprietary Formats:** Unlike standardized media formats such as JPEG or MP4, radar data lacks a universal file format. Vendors adopt proprietary representations **Texas Instruments** commonly employs binary Type–Length–Value (TLV) structures, while **Google** relies on internal tensor based formats. This fragmentation creates significant challenges for forensic

analysis and necessitates the development of opensource parsers, such as mm Wave capture libraries, to decode proprietary data blobs into interpretable structures suitable for evidentiary examination[16].

- **Privacy vs. Surveillance:** Radar's ability to sense activity through walls raises significant privacy and civil liberties concerns[29]. As next generation 6G networks converge sensing and communication through Integrated Sensing and Communication (ISAC), wireless infrastructure itself is poised to function as a distributed radar system[29]. In this context, forensic practice must carefully balance the investigative value of radar derived data against constitutionally protected privacy rights. Investigators must adhere to strict purpose limitation principles embedded in modern data protection regimes, ensuring that such data is collected, analysed, and used only within clearly defined and legally justified boundaries[29][30][35].

8 Conclusion

Although there is a potential, there are major challenges.

- **Data Volatility:** IoT devices often have a small onboard memory and the high bandwidth radar data is often only held in circular buffers before being overwritten. Without instantaneous live acquisition or approved forensic preparedness plans like automated event synchronization with cloud storage key evidentiary information can be irrecoverably lost in a few minutes.

- **Proprietary Formats:** Radar data has no standard file format unlike the standardized media formats including the JPEG or MP4. Vendors In use of proprietary representations typical of Texas Instruments binary Type Length Value (TLV) structures, and Google on in-house tensor based representations. The resulting fragmentation poses substantial problems to forensic investigation and methods to decode proprietary data blobs to interpretable format appropriate to support evidentiary analysis must be developed, e.g. mm Wave capture libraries[16].

- **Privacy vs. Surveillance:** The fact that Radar can detect the presence of an individual behind a wall brings up the question of privacy and civil liberties. With next generation 6G networks forming sensing and communication merged with Integrated Sensing and Communication (ISAC), wireless infrastructure in itself can be a distributed radar system. In this respect, the forensic practice should maintain a cautious equilibrium between the investigative worthiness of radar obtained data and the constitutionally acknowledged privacy. The investigators should comply with strong principles of purpose limitation in the context of modern data protection regimes, so such data should be obtained, processed, and utilised within the frames of well-defined and legally justified limits[30][35].

Acknowledgement

The author acknowledges the support of Mr. Prasanna Kumar (Faculty of IoT) and Mr.

Dhanunjaya Rao (Faculty of Digital Forensics) of the School of Science (SoS), Digital Forensics Department, Malla Reddy University, Hyderabad, for providing the necessary academic resources and infrastructure to conduct this research.

Conflict of Interest

I declare that I have no conflicts of interest related to this research. I have no personal or financial relationships that could influence my work.

References

1. Qorvo. (n.d.). *Ultra-Wideband (UWB) Radar: Beyond Ranging to Advanced Sensing*. Retrieved from https://www.qorvo.com/designhub/blog/ultrawidebanduwbradarbeyondrangingtoadvancedsensing.11
2. Talking IoT. (2024). *A New Frontier: UWB Radar*. Retrieved from https://talkingiot.io/anewfrontieruwbradar/.13
3. Yarici, A., et al. (2023). "Human Detection and Tracking via Ultrawideband UWB Radar". *ResearchGate*..15
4. Sesyuk, A., et al. (2024). *Comparative Analysis of 3D Sensing with mmWave and 3D Positioning with UWB*. Lancashire Knowledge..14
5. De Witte, P., et al. (2024). "Exhaustive Survey of UWB Radar Technology". *arXiv preprint arXiv:2402.05649*..12
6. Wang, S., et al. (2016). *Deep Soli: Gesture Recognition using 60GHz Radar*. GitHub Repository..25
7. Google Research. (2020). *Soli RadarBased Perception and Interaction in Pixel 4*. Google AI Blog..22
8. University of St Andrews. (2016). *RadarCat: Exploiting Google's Soli Radar for Object Recognition*..27
9. Anritsu. (n.d.). *Automotive Radar Sensors for ADAS and Autonomous Vehicles*..3
10. CarADAS. (2024). *What is an ADAS Radar Sensor?* Retrieved from https://caradas.com/adasradarsensor/.4
11. Zhang, Y., et al. (2024). *WiFi CSI Based Human Activity Recognition*. MDPI Sensors..8
12. Ministry of Law and Justice. (2023). *The Bharatiya Sakshya Adhiniyam, 2023*. Government of India..69
13. Chen, V. C. (2019). *The MicroDoppler Effect in Radar*. Artech House..2
14. Tesla. (2024). *Privacy and Vehicle Data*. Retrieved from https://www.tesla.com/support/privacy.30
15. Texas Instruments. (2021). *DCA1000EVM Data Capture Card User's Guide*..36
16. Yan, H., et al. (2022). "Toward SpoofingResilient mmWave Radar Sensing". *ResearchGate*..60
17. Komal. (2025). "The Bharatiya Sakshya Adhiniyam: A Framework for Admitting Electronic Evidence". *IJLSSS*..7
18. Corpotech Legal. (2024). *Admissibility of Electronic Evidence under Section 63 BSA*..70
19. Robin Radar. (2024). *CounterDrone Radar Technologies*..71

20. Strohmayer, J., & Kampel, M. (2023). *WiFi CSIBased LongRange ThroughWall Human Activity Recognition*. Zenodo..34
21. MathWorks. (2024). *I/Q Data Collection and Detection Generation with TI mmWave Radar*. MATLAB Documentation..72
22. Graff, T., et al. (2023). *FMCW Radar Spoofing and Parameter Estimation*. RadioNav Lab..10
23. Naha, A., et al. (2022). *Detection of Replay Attacks in CyberPhysical Systems*..64
24. Gadzhovski. (2024). *TRACE Forensic Toolkit*. GitHub..73
25. Zhu, H., et al. (2024). *Comparison Between WiFiCSI and RadarBased HAR*. IEEE Xplore..35
26. Li, X., et al. (2024). *CrossScene Human Activity Recognition Based on Radar and WiFi Multimodal Fusion*. MDPI..51
27. Wang, Y., et al. (2020). *Experimental Comparison of IRUWB Radar and FMCW Radar for Vital Signs*. PubMed..19
28. Aljahdali, S., et al. (2021). *IoT Forensic Taxonomy and Interaction*. ResearchGate..74
29. Magnet Forensics. (2024). *Overcoming Key Challenges in Remote Data Collection*..75
30. Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023*. Government of India..68
31. ApniLaw. (2023). *Section 63 – Bharatiya Sakshya Adhiniyam, 2023*..57
32. Ni, Z., & Huang, Y. (2022). *GaitBased Person Identification and Intruder Detection Using mmWave Sensing*. ResearchGate..17
33. Pegoraro, J., et al. (2023). *Multipathassisted WiFi sensing*. arXiv..76
34. PCISIG. (2021). *PCI Express Base Specification Revision 6.0*. PCISIG..36
35. Infineon Technologies. (2024). *RadarBased Human Activity Recognition in PrivacySensitive Environments*. PMC..37
36. MIT Lincoln Laboratory. (2020). *Forensic Detection of Tampered Radar I/Q Data*. MIT DSpace..