Chapter 2 of this thesis provides an extensive literature review that delves into the existing knowledge surrounding the topic of ”Post-Crime Detection and Tracking of Criminals Using Sensor Data Pattern Analysis.” In this chapter, we thoroughly examine and analyze a broad spectrum of scholarly articles, research papers, books, and other pertinent sources that relate to crime detection, sensor data analysis, and the integration of the Internet of Things (IoT) in law enforcement. By immersing ourselves in the available literature, this chapter seeks to establish a robust foundational understanding, pinpoint research gaps, and unearth the principal methodologies and approaches previously employed in this domain. The insights drawn from this literature review will form a guiding framework for the subsequent phases of this thesis, ultimately enriching our comprehension and exploration of the potential embodied in sensor data pattern analysis for post-crime detection and criminal tracking.

In 2012, Lewis undertook a study that delved into the challenges faced by communities as a result of criminal activities, and subsequently developed a technological solution with the goal of analyzing and preventing such crimes [29]. This study holds a pivotal place in the landscape of criminal investigation and prevention technologies. The research underscores that effective strategies for crime prevention hinge on a comprehensive understanding of two key components: victimization and control strategies. The first facet, victimization, involves grasping the contextual details of the crime, encompassing the victim, the perpetrator, and the surrounding environment. By gathering and analyzing such data, valuable patterns and insights can be gleaned, contributing to the prevention of similar crimes in the future. The study further accentuates the importance of comprehending the communities from which both the victim and the offender originate, as community dynamics significantly shape individuals’ behavior.

With a primary focus on harnessing technology to curtail crime rates, the study aimed to cultivate community participation in discussions and initiatives centered on crime prevention, particularly in urban areas. To achieve this, a system was devised that allowed individuals to report criminal incidents within their neighborhoods, enabling collaborative efforts against crimes through easily accessible technology available to the general public.

The study aimed to explore the challenges faced by a community in Trinidad and Tobago as a result of crime and violence, and how technology can be used to enhance learning and crime prevention. The study used a mixed-methods approach, combining quantitative and qualitative data collection and analysis. The study found that technology can play a positive role in facilitating learning and crime prevention, but it also requires adequate infrastructure, training, and support. The study also suggested some recommendations for improving the use of technology in the community.

Anderez et al. [30] provide a comprehensive exploration of the evolving land scape of crime prevention through the lens of technological innovations. This part of the thesis discusses various aspects crucial to understanding and implementing technology-driven solutions for crime prevention. Their work delves into the diverse range of technologies, from short-range communication to machine intelligence systems, evaluating their potential adoption in crime prevention. It underscores the significance of considering societal, ethical, and privacy implications in the development and deployment of these technologies. The challenges associated with adopting technological innovations are thoroughly examined. Issues such as data integrity, battery life, accuracy, affordability, and technology misuse are discussed in detail. The document emphasizes the need for meticulous data collection, considering diverse populations, and ensuring the integrity of data throughout its life cycle.

The Venn diagram presented in figure 2.1 illustrates the intricate relationships

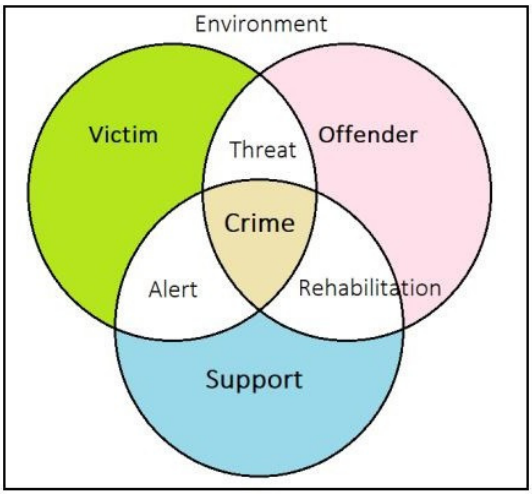

Fig. 2.1: A Venn diagram showing the relationship between victim, threat, and defender in the context of crime

among three central stakeholders in the realm of crime: victims, threats, and defenders [30]. Each entity plays a distinct role—the victim endures harm, the threat perpetrates the crime, and the defender endeavors to shield the victim from harm. The diagram adeptly portrays the potential intersections between these groups, emphasizing that a victim might also pose a threat, or a defender may become a threat under certain circumstances. Notably, there exist areas beyond overlap where each group functions independently, such as victims unthreatened, threats non-victimizing, and defenders without a specific victim to protect.

This conceptualization is pivotal in crafting effective crime prevention and response strategies. Analyzing the factors contributing to the overlap allows for the development of targeted interventions to mitigate the occurrence of crimes. The subsequent breakdown of examples, ranging from victims engaged in gang violence to defenders who may inadvertently become threats, offers practical insights. Whether it be victims resisting arrest or defenders not directly protecting a specific victim, comprehending these dynamics enables a nuanced approach to crime prevention. Ultimately, this understanding of the intricate relationships informs strategies that better safeguard the public and reduce the likelihood of criminal incidents.

These early investigations exemplify the strides taken in the domain of criminal investigation and prevention technology, with a distinct focus on utilizing technology to amass data from users and furnish them with a platform to engage in proactive discussions and deter crimes. Another noteworthy contribution, presented by Agangiba et al. (2013)[31], encompassed the creation of a mobile device tailored for the identification and reporting of crimes in metropolitan areas. Recognizing the challenge of delayed communication with law enforcement due to resource constraints, the researchers devised a mobile application enabling individuals to upload details of criminal incidents and promptly alert the police via the app. This real-time exchange aimed to facilitate law enforcement’s rapid apprehension of wrongdoers. The data collected through the application was transmitted to a distant server, housing information regarding criminal sightings, stolen items, and trends. Subsequently, this dataset was harnessed to provide insights to the police, enhancing crime prevention and response strategies.

In 2014, Agangiba et al. [31] introduced a groundbreaking system utilizing geolocation to develop an emergency response mobile application that seamlessly connected with command centers. This innovative application was accessible through both mobile and web interfaces and served to promptly alert ambulances, police, and fire departments in case of emergencies. By leveraging the Global Positioning System (GPS) on users' phones, the application accurately determined their locations and transmitted this critical information to emergency services. Moreover, it efficiently transferred additional data such as the user's name, age, and location to the central command system. This pioneering use of the Internet of Things (IoT) marked an early application that aimed to prevent crimes by instantly notifying law enforcement and emergency services.

In 2015, Fernando [32] created a mobile application named "Street Watch" aimed at addressing street crimes and providing safety solutions. This Android application sent real-time notifications to users regarding ongoing crimes in their vicinity, which were updated by fellow app users. Moreover, it empowered individuals to swiftly alert authorities if they encountered assault or emergency situations. The app not only gathered crucial data about areas prone to criminal activities but also facilitated user vigilance, allowing them to steer clear of high risk zones. Additionally, the application furnished comprehensive details about nearby police stations, contributing to bolstered safety measures for its users. By merging technology and community involvement, Fernando's app emerged as a proactive tool in preventing crime and ensuring public safety.

In 2016, Jeon and Jeong [33] embarked on the development of a crime prevention system that harnessed the power of big data and IoT (Internet of Things), as illustrated in figure 2.2. During this era, the convergence of big data and IoT was gaining notable traction. The researchers recognized a limitation in conventional surveillance setups, such as CCTV cameras, which often lacked the ability to swiftly notify authorities upon detecting suspicious incidents. In response, they introduced an innovative solution that leveraged data derived from public crime recording devices, subsequently issuing alerts to individuals based on this accumulated data. The operational mechanism of their system unfolds as follows: Primarily, the system collates data from various crime recording devices. Subsequently, this amassed data is

subject to analysis through a comparative assessment with an extensive repository of information (big data), gauging the gravity of the detected offense. Depending on the severity and characteristics of the incident,

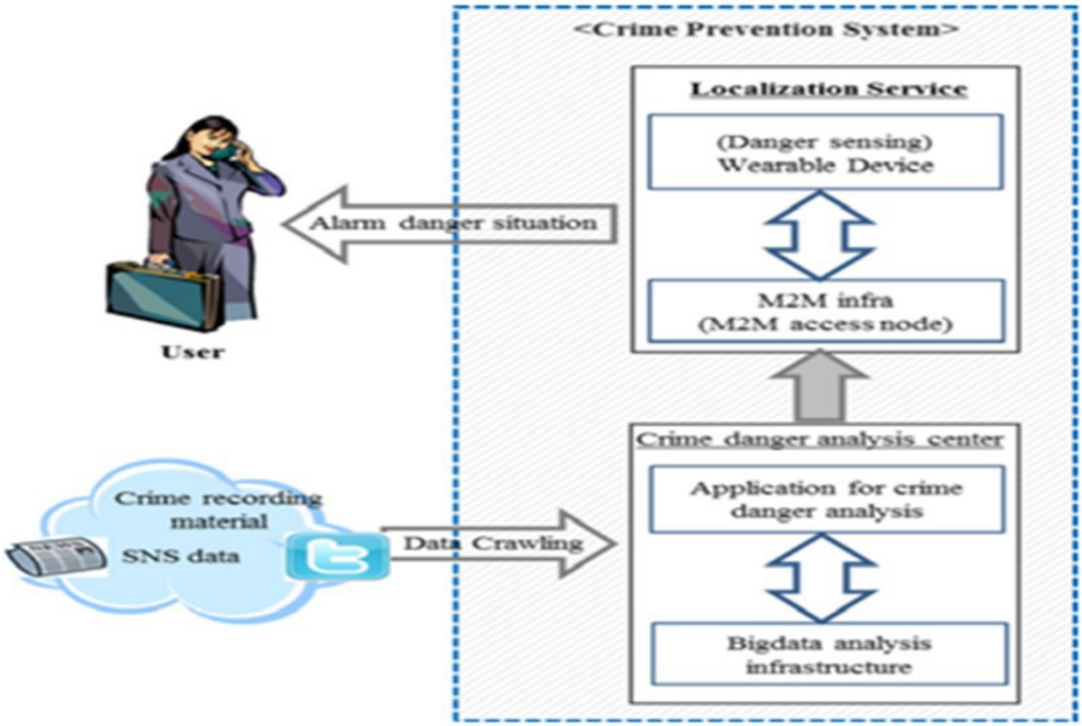

Fig. 2.2 : Big data and IoT interface [33]

notifications are dispatched to users' mobile devices. These mobile devices, in turn, engage with a wearable sensor apparatus to proactively alert users to potential criminal scenarios, fostering heightened vigilance and ensuring personal safety.

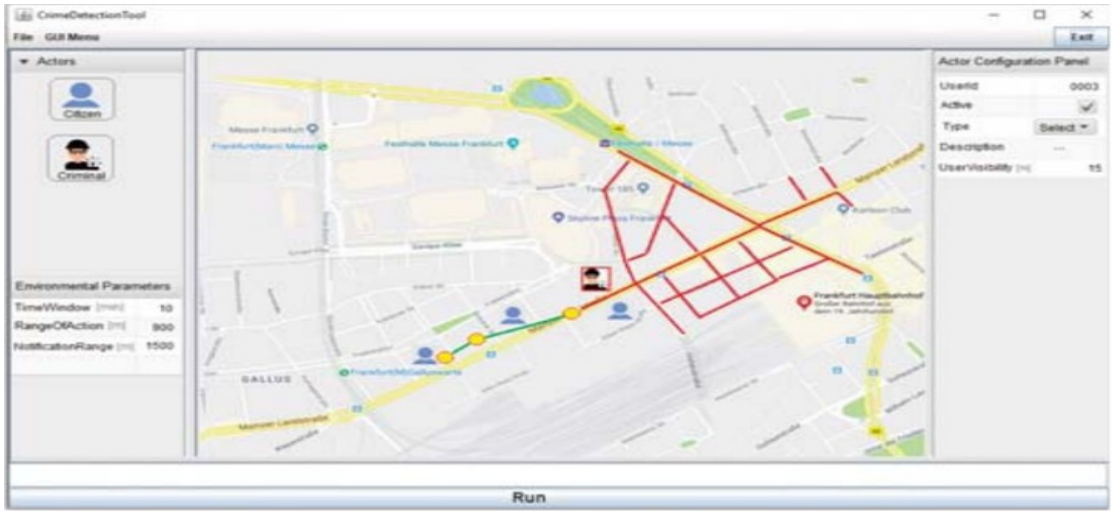

Fig. 2.3: IoT application developed for criminal tracking. The predicted routes the criminal could take based on the place where the crime occurred is found. [34]

In 2019, an innovative endeavor by Tundis, Kaleem, and Muhlhauser showcased a state-of-the-art device harnessing IoT sensors for criminal activity tracking [34]. The primary aim of their study was to foster improved communication between the public and the police within urban settings. To realize this goal, they devised a multi-layered mobile application (depicted in figure 2.3) comprised of IoT, edge, and analysis layers. The IoT layer encompassed users' devices, which gathered pertinent data. The edge layer acted as an intermediary, aggregating user data and channeling it to the cloud for further processing. Finally, the analysis layer delved into reported crimes, generating potential solutions to enhance police responsiveness. Moreover, the application capitalized on GPS within users' devices to share their precise locations with law enforcement. For comprehensive testing, the researchers incorporated a simulation mode utilizing virtual actors to replicate criminal scenarios. This facilitated the identification of potential solutions and predictions regarding the perpetrators' possible routes, thereby aiding efficient police tracking. This inventive application sought to instigate proactive crime prevention strategies and enhance the efficacy of law enforcement responses. In 2021, AlDahoul, Karim, Datta, Gupta, Agrawal, and Albunni unveiled a convolutional neural network (CNN) fortified by IoT sensors for the detection of violent activities [35]. Employing a Long Short Term Memory (LSTM) network on a Raspberry Pi device, the team harnessed video data from diverse surveillance sources, including CCTVs. Spatial features extracted from video frames enabled the model to classify actions within these frames as either violent or non-violent. The training and validation phases capitalized on open source datasets, namely RWF-2000 and RLVS-2000, encompassing videos from streets, schools, and correctional facilities. Remarkably, the model attained an accuracy of 72.35%. This approach empowers compact IoT devices to discern criminal activities from video feeds sourced from diverse urban locations. By promptly alerting local law enforcement to potential violent incidents, this method engenders a proactive response to security concerns.

In recent times, IoT-based research has witnessed notable strides. Tundis, Uzair, and Muhlhauser (2022) introduced an ingenious context aware model harnessing IoT technology for crime detection [36]. This approach entailed scrutinizing body posture, stress levels, and GPS data to prognosticate both the occurrence and site of a crime. A

smartwatch, paired with a mobile phone, facilitated data collection. Researchers developed a machine learning model proficient in discerning user body posture from smartwatch data. The identification of heightened stress levels was supported by a predefined threshold; surpassing this threshold indicated elevated stress. All accumulated data underwent processing within a mobile application, which promptly alerted the police upon detecting potential criminal activities. This revolutionary system presents promising avenues for amplifying crime detection and facilitating swift responses via IoT-driven technological advancements.

Ferreira *et al.*[37] have conducted an extensive survey on various electrochemical sensors and their applications in forensic science. Their comprehensive report explores the potential of these sensors across different forensic domains, highlighting the growing importance of advanced sensing technologies in criminal investigations and evidence analysis.

In a related study, Meffert *et al.*[38] have developed an innovative forensic state acquisition system that leverages the Internet of Things (IoT). Their research utilized an IP camera and integration hub for thermostat control, demonstrating the potential of smart home devices in forensic contexts. Through rigorous cloud testing, they identified multiple scenarios that could yield valuable forensic insights, with a particular emphasis on door lock activities and motion sensor data. The primary objective of their work was to establish a robust framework compatible with a wide range of IoT devices, showcasing the potential of smart home technology in digital forensics. In contrast to their approach, our research aims to harness the capabilities of mobile phones as IoT devices themselves, eliminating the need for separate IoT sensors and potentially simplifying the forensic data collection process.

Mylonas et al.[39] have provided a comprehensive overview of various smartphone based forensic techniques, shedding light on the evolving landscape of mobile device forensics. Their work not only summarizes these techniques but also delves into the practical applications of smartphone-based evidence in legal proceedings.

By exploring the legal implications of such evidence, their research underscores the critical role that mobile devices play in modern forensic investigations and high lights

the need for robust methodologies in extracting and analyzing data from these ubiquitous devices.

In an effort to enhance digital image forensics, Lekshmi *et al.*[40] have developed a sophisticated SVM-based algorithm capable of classifying and identifying source cameras. Their innovative approach combines EXIF information with sensor pattern noise analysis to pinpoint the exact camera used for image acquisition. The study encompassed a diverse set of seven different cameras and took into account photo response non-uniformity noise, demonstrating the algorithm's versatility and robustness. Drawing inspiration from their groundbreaking work, our research is exploring the potential of incorporating temperature sensor data as a key feature parameter. We hypothesize that temperature sensors can provide unique environmental noise pattern information, potentially offering an additional layer of forensic evidence. This approach could significantly enhance our ability to authenticate and trace the origin of digital images, contributing to the broader field of digital forensics and cyber security.

Malik *et al.*[41] introduced a network behavior examination method for verifying mobile device forensics. While they couldn't differentiate forensic artifacts based on mobile operating systems, they successfully identified behavior patterns in certain devices related to actions like ICMP packet transmission and streaming video reception. Their approach determines whether mobile data is actively generated by the user or passively generated by the device.

Jahangiri *et al.*[42] employed mobile sensor data for identifying transportation modes (e.g. air travel, rail travel etc.) using KNN, SVM, and tree-based classifiers. In a similar vein, we aim to collect mobile sensor data, but our primary objective is to detect suspicious activities rather than transportation modes.

Rosser *et al.*[43] employed mobile phone sensor data to construct interiors and generate 3D models. Their method interactively captured the source scene using smartphone sensors. While their focus wasn't on suspicious activities, we believe our work could also potentially predict future criminal scenes using available sensor data.

Khan *et al.*[44] developed a human identification system classifying human motions based on mobile phone sensors such as accelerometers, gyroscopes, and

magnetometers. Their system achieved an accuracy of 96.5% in distinguishing between normal walking and brisk walking.

Horwitz *et al.*[45] designed a system predicting depression and suicidal ideation among medical interns using Fitbit data. Although their work centered on mood prediction, it demonstrated that relying solely on Fitbit data might not be sufficient for predicting mood-related outcomes.

Ouguz *et al.*[46] developed a human identification system based on accelerometer data from mobile sensors. They achieved 99% accuracy in recognizing humans using accelerometers and utilized KNN and RNN for classification. Our work goes beyond accelerometers, incorporating gyroscope and other mobile sensors.

Pradhan *et al.*[47] devised a classification system using wearable sensor technology. Their goal was to create reliable IoT technology capable of distinguishing health data from communication data. Their system showed a failure rate improvement of around 10%, with response and processing times of 0.9 seconds and 454 milliseconds, respectively.

Wampfier *et al.*[48] developed a system predicting affective states using smart phone sensors, including touch and heat maps. They achieved accuracy levels of up to 70% through a combination of keystrokes, gyroscopic, and linear acceleration measurements.

In 2019, Tundis and colleagues proposed an IoT sensor based technique for detecting and tracking criminals [34]. Their approach facilitated communication between authorities and the public through a mobile application. The application was structured into multiple layers, each with distinct functions. The first layer, known as the IoT layer, encompassed user owned devices. The second, the edge layer, served as an intermediary for data collection and storage, transferring data to the cloud. Lastly, the analysis layer utilized the collected data to perform analysis, yielding detailed crime results.

In 2012, Lewis conducted a study on the impact of crimes on communities, exploring crime investigation and mitigation techniques. The study aimed to reduce urban crime rates by leveraging existing technology and fostering public awareness. This

culminated in the design of technologies accessible to the general public for crime prevention.

Okmi et al. [49]discusses about the use of mobile phone data in crime applications. It discusses the different types of mobile phone data that can be used, such as call detail records, location data, and social media data. The article also discusses the different ways that this data can be used to fight crime, such as predicting crime hotspots, identifying criminals, and tracking offenders. The authors conclude that mobile phone data is a valuable tool for fighting crime, but that there are also some challenges that need to be addressed, such as privacy concerns and the need for more standardization. The figure 2.4 outlines the diverse levels at which mobile phone data can be collected, emphasizing individual, aggregated, and cell tower levels[49]. At the individual level, data provides a granular view of a user's behavior, including call logs, text history, app usage, and location data. This enables insights into personal routines, social networks, and travel habits. Aggregated data, sourced from groups of users, unveils general behavior patterns in populations, aiding in the identification of trends like traffic flows, crime concen-

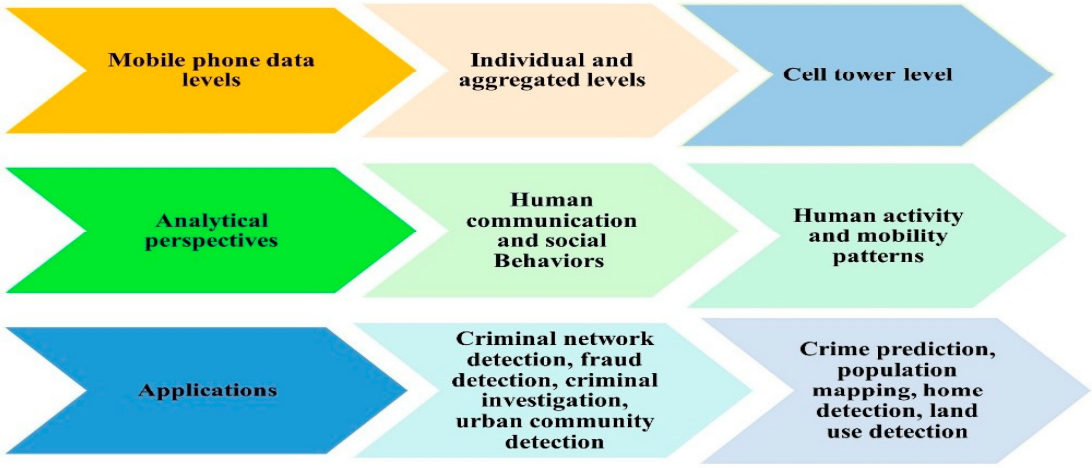

Fig. 2.4: Multiple analytical perspectives and applications based on mobile phone data.

trations, and overall population movements. Cell tower level data encompasses all users connected to a specific tower, offering a broader perspective on area-wide activities, such as the number of people and their presence times. From an analytical standpoint, the document introduces various perspectives for mobile phone data

analysis. These include understanding human mobility patterns, communication behaviors, social interactions, and mobile phone usage activities. Each perspective provides unique insights into different aspects of human behavior, ranging from tracking movements and identifying social networks to understanding communication patterns and detecting fraudulent activities. The applications of mobile phone data are wide-ranging. Notably, it can be employed in crime prediction and prevention, public health monitoring, urban planning, transportation analysis, as well as marketing and advertising strategies. By utilizing mobile phone data comprehensively, researchers and professionals can gain a multifaceted understanding of human behavior, enabling informed decision making across various domains. Figure 2.5 gives an overview of comparing various methods and problems encountered in mobile phone data studies[49]. Key challenges are categorized as classification, clustering, detection, mapping, and privacy concerns. Classification involves predicting user categories or behaviors; clustering groups users based on similarities;

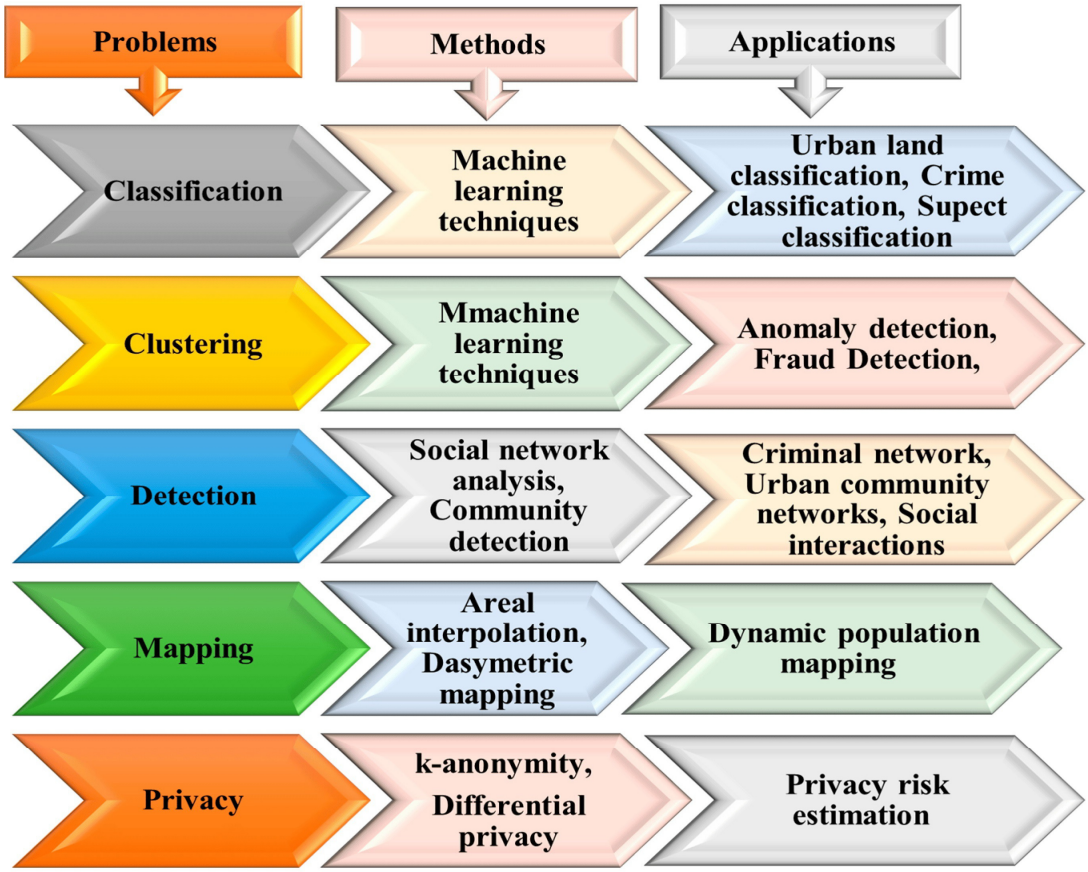

Fig. 2.5: Comparison of different methods and problems used in mobile phone data studies

detection identifies events or patterns; mapping visualizes data on a map; and privacy addresses user data protection. The methods introduce powerful tools for addressing the mentioned problems. Machine learning emerges as a versatile approach applicable to classification, clustering, detection, and mapping. Social network analysis delves into studying social connections between users, offering insights into social groups and potential unrest. Areal interpolation techniques are highlighted for mapping mobile phone data, especially useful in visualizing population density, traffic patterns, and crime hotspots. Differential privacy is presented as a crucial technique to safeguard user privacy during data collection and analysis. The applications gives practical implementations of mobile phone data studies are outlined. Urban land use classification emerges as an application, aiding in the classification of land use in urban areas for future development planning and monitoring changes over time. Crime classification involves using mobile phone data to categorize crime incidents, identifying hotspots, predicting crime patterns, and tracking offenders. Suspect classification is also introduced, leveraging mobile phone data to classify suspects in criminal investigations, focusing investigative efforts on those more likely to be guilty.

Agangiba in (2013) [31] designed a device to detect and report crimes. This mobile device allowed users to upload evidence and contact the police through a mobile application. The data was transmitted to a remote server, enabling prompt police intervention and notifying them about recurring offenders.

Fernando developed the ”Street Watch” mobile application that monitored streets and enabled users to report crimes, alerting both the police and nearby users about criminal activities [32]. The application also stored historical crime data, alerting users entering crime prone areas.

In 2016, Jeon and Jeong [33] designed a crime prevention system utilizing big data and IoT. Their approach involved collecting crime data from public sources, comparing recorded incidents against a reference to gauge severity. Users were notified of crime levels via phones or wearable sensor devices.

In 2021, AlDahoul, Karim, Datta, Gupta, Agrawal, and Albunni [35] developed a violence detection system using LSTM based IoT nodes. They executed the Long

Short Term Memory algorithm on a Raspberry Pi, extracting information from various video types. Using RWF-2000 and RLVS-2000 datasets for training and validation, their model achieved an accuracy of approximately 73%, triggering alerts to authorities.

Al et al. [50] conducted a comprehensive review of Mobile Forensics Investigation Process Models (MFIPMs) within the realm of Mobile Forensics (MF). Their focus centered on the recovery of Potential Digital Evidence (PDE) from mobile devices using forensic methodologies. Their objective was to illuminate the evolutionary trajectory of the MF domain and pinpoint both current and prospective challenges. Through the examination of 100 MFIPMs, they proposed a cohesive framework called the Harmonized Mobile Forensic Investigation Process Model (HMFIPM) to standardize and structure investigative processes in the MF domain.

Teing et al. [51] addressed the intricate challenges posed by cloud forensics due to the exponential surge in data volume, diversity, and speed. Emphasizing the importance of digital forensic practitioners staying abreast of relevant data artifacts recoverable from cloud products under scrutiny, they specifically delved into CloudMe, a prominent cloud storage service. Their research delineated artifact types and locations associated with CloudMe client application installation and uninstallation, login and logout events, and file synchronization from both computer desktop and mobile clients. The insights garnered from this study are poised to inform the development of future tools and techniques, including data mining approaches, for comprehensive cloud enabled big data endpoint forensic investigations.

Kim et al. [52] introduced the Mobile Forensic Reference Set (MFReS) as a systematic mobile forensic investigation procedure and tool. The MFReS functions as an aggregation of repositories, databases, and services, facilitating efficient data retrieval from databases for meaningful categorization of crime related data among a myriad of data types found in mobile devices. The MFReS aptly analyzes information from installed applications and user behavior, incorporating system data, application data, and multimedia data. Their developed tool offers investigators the capacity to analyze log files of all applications, decipher behavior along timelines, geographical data, and other distinctive attributes. This research contributes to the advancement of

mobile forensic support systems and outlines a path for the development of mobile data analysis tools.

Mumba et al. [53] undertook an exploration of the intricate challenges posed by mobile forensic investigations in the rapidly evolving landscape of mobile device technology. Acknowledging the crucial role of mobile devices as sources of digital evidence, the authors highlighted the complexity of performing forensically sound data acquisition from these devices. Through a case study, they aimed to evaluate the efficacy of a Harmonized Digital Forensic Investigation Process (HDFIP) as outlined in the ISO/IEC 27043 draft international standard. Their focus was on extracting potential digital evidence from mobile devices, assessing the HDFIP's effectiveness in mobile forensic investigations, and identifying areas for warranting improvement.

2.1 Recent cases solved due to mobile phone activities

The use of mobile phone data in crime solving is a growing trend, often sparking debates about privacy and effectiveness. Here are some recent examples where it played a key role:

Solving missing person cases:

- **Idaho Murders:** Cell phone data traced suspect Bryan Kohberger's movements on the night of the murders, placing him near the crime scene and establishing a possible timeline.
- **Utah Couple Disappearance:** Analyzing call records helped locate a missing couple who had fallen while hiking. Cell tower pings led search teams to their remote location.

Apprehending violent criminals:

- **Baltimore Shootings:** Ballistic evidence combined with cell phone location data identified suspects involved in a series of shootings, leading to their arrest.
- **Maryland Carjacking:** Tracking a stolen phone's signal led police to the suspect and recovered the stolen vehicle.

Exposing organized crime:

- **Italian Mafia Crackdown:** Authorities used cell phone records to map communication networks within the mafia, revealing hierarchies and facilitating arrests of key members.

- **Mexico Drug Cartel Bust:** Mobile data analysis exposed communication connections between cartel members, disrupting their operations and leading to numerous arrests.

It's important to note that these examples are just a snapshot. Mobile phone data is used in countless investigations every day, with varying degrees of success and raising ongoing ethical concerns.

Here are some additional points to consider:

- **Legal hurdles:** Obtaining warrants for access to mobile phone data often requires demonstrating relevance to a specific crime.
- **Accuracy and limitations:** Location data from cell towers can be imprecise, and not all activities leave a digital trace.
- **Privacy concerns:** The use of such data raises privacy concerns, prompting debates about balancing security with individual rights.

Recent cases related to mobile phone activities and cybercrime in India. Financial frauds account for over 75 % of cybercrimes in India from January 2020 till June 2023. Nearly 50 % of these cases are related to UPI (Unified Payments Interface) and internet banking tracked down from mobile phones. The number of cyber crimes reported in India has been on the rise. In 2022, the state with the highest number of reported cyber crime cases was Delhi, and it's essential to stay vigilant and cyber cell took necessary precautions. Cyber stalking and bullying cases were solved using mobile phone data, reported across various states in India. In May 2021, there was a significant data breach involving Air India, which was later revealed from mobile phone data. Such incidents highlight the risks associated with third party vulnerabilities. India has been investing in cyber security to combat threats using mobile sensor data. The expenditure towards cyber security in 2019 was substantial, with a forecast for further investment in 2024. The use of mobile phone data in crime solving is a complex issue with both benefits and drawbacks. As technology evolves, it's crucial to have open discussions about its usage while striving to ensure both effective law enforcement and respect for individual privacy.

Mobile phone data is also a valuable source of digital evidence that can help investigators, to solve crimes. Here are some recent examples of how mobile phone data is used in crime applications:

A systematic review of mobile phone data in crime applications found that mobile phone data can be used to detect suspicious activities, identify criminal networks, predict crime, and understand human communication and mobility patterns in urban sensing applications [49]. A Medium article explained how police use cell phones and video surveillance to establish location, timeline, and identify everyone who was in a given area during a particular time. Mobile phones can also show a victim's contacts and conversations leading up to a crime [54]. A 'India Today' report revealed how police use Google location data to track cell phones and investigate crimes. A warrant launches a three step process, which starts with the tech giant providing anonymous information and can progress to include names and emails connected to a subset of targeted phones [55]. Many reports discussed the challenges and opportunities of using digital data from personal devices in criminal investigations. The authors argued that there is a need for clear and consistent legal frameworks and ethical guidelines to balance the privacy rights of citizens and the public safety interests of law enforcement [56]. An Interesting Engineering article highlighted how cell phone tracking is increasingly being used to solve crimes. The article cited examples of how cell phone tracking helped catch serial killers, kidnappers, and terrorists[57]. The article also mentioned some of the limitations and risks of cell phone tracking, such as false positives, hacking, and misuse [49].

Dawre et al. provide a comprehensive overview of the digital forensic process and tools available for investigating crimes committed using mobile devices and computers [58]. They highlight the continued growth of the mobile device market and its potential use in criminal activities, emphasizing the diverse range of manufacturers and models available in the market. The authors discuss the increasing dependence of people on applications such as SMS, MMS, Internet access, and online transactions, which further adds to the complexity of digital forensics. They point out that the variety of tools and techniques available for identifying and investigating crimes committed with the help of mobile devices or computers can make it challenging for professional investigators to select the appropriate forensic tools for seizing internal

data from these devices. Moreover, the authors emphasize the importance of mobile devices as a valuable source of evidence for forensic investigators to either prove or disprove the commission of crimes by victims. They also provide insights into popular digital forensic tools and offer an in depth analysis for investigators to choose between free sources or commercial tools based on their specific needs. Furthermore, Dawre et al. compare computer forensics with mobile forensics, highlighting the differences in techniques and tools used for investigating crimes committed using these devices. They also explore the various areas and applications of digital forensics, showcasing the wide range of domains in which these techniques are applicable.