applied sciences

Review

A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques

Amjed Ahmed Al-Kadhimi [1,2], Manmeet Mahinderjit Singh [1,*] and Mohd Nor Akmal Khalid [3]

[1] School of Computer Sciences, Universiti Sains Malaysia, Georgetown 11800, Penang, Malaysia; amjed.alkadhimi@student.usm.my
[2] Computer Engineering Department, University of Basrah, Basrah 64001, Iraq
[3] School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi 923-1211, Japan; akmal@jaist.ac.jp
* Correspondence: manmeet@usm.my

Abstract: Advanced persistent threat (APT) refers to a specific form of targeted attack used by a well-organized and skilled adversary to remain undetected while systematically and continuously exfiltrating sensitive data. Various APT attack vectors exist, including social engineering techniques such as spear phishing, watering holes, SQL injection, and application repackaging. Various sensors and services are essential for a smartphone to assist in user behavior that involves sensitive information. Resultantly, smartphones have become the main target of APT attacks. Due to the vulnerability of smartphone sensors, several challenges have emerged, including the inadequacy of current methods for detecting APTs. Nevertheless, several existing APT solutions, strategies, and implementations have failed to provide comprehensive solutions. Detecting APT attacks remains challenging due to the lack of attention given to human behavioral factors contributing to APTs, the ambiguity of APT attack trails, and the absence of a clear attack fingerprint. In addition, there is a lack of studies using game theory or fuzzy logic as an artificial intelligence (AI) strategy for detecting APT attacks on smartphone sensors, besides the limited understanding of the attack that may be employed due to the complex nature of APT attacks. Accordingly, this study aimed to deliver a systematic review to report on the extant research concerning APT detection for mobile sensors, applications, and user behavior. The study presents an overview of works performed between 2012 and 2023. In total, 1351 papers were reviewed during the primary search. Subsequently, these papers were processed according to their titles, abstracts, and contents. The resulting papers were selected to address the research questions. A conceptual framework is proposed to incorporate the situational awareness model in line with adopting game theory as an AI technique used to generate APT-based tactics, techniques, and procedures (TTPs) and normal TTPs and cognitive decision making. This framework enhances security awareness and facilitates the detection of APT attacks on smartphone sensors, applications, and user behavior. It supports researchers in exploring the most significant papers on APTs related to mobile sensors, services, applications, and detection techniques using AI.

Keywords: cyber cognitive situational awareness (CCSA); Joint Directors of Laboratories (JDL); MITRE framework; user behavior; spear phishing; game theory

Citation: Al-Kadhimi, A.A.; Singh, M.M.; Khalid, M.N.A. A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques. *Appl. Sci.* **2023**, *13*, 8056. https://doi.org/10.3390/app13148056

Academic Editor: Valentino Santucci

Received: 11 May 2023
Revised: 16 June 2023
Accepted: 22 June 2023
Published: 10 July 2023

1. Introduction

Advanced persistent threat (APT), which differs significantly from traditional network attacks, has emerged recently. Cyber attacks, or APTs, known for their ability to steal intellectual property, disrupt critical infrastructure, or cause millions of dollars in damages, are a growing concern [1]. In contrast, traditional network attacks have been employed as cyber attacks for many years to compromise computer network security and steal sensitive information. These attacks exploit network systems and protocol vulnerabilities to gain unauthorized access to networks, steal confidential data, or disrupt normal network operations. The common types of traditional network attacks are denial-of-service (DoS), man-in-the-middle (MITM), sniffing, phishing, and structured query language (SQL) injection [2,3].

According to Powerful Growth, the global APT protection market is expected to reach USD 20,290.7 million by 2027, expanding at a 20.9% compound annual growth rate (CAGR). The global APT defense market is estimated to rise rapidly throughout the forecast period, given the exponential growth of cyber attacks globally, including malware and APTs [4]. Thus, APT is an important threat to be mitigated in mobile and computer systems.

Deliberate, repetitive, and covert cyber attacks that target specific companies rather than random individuals or regular system users are a defining characteristic of APTs [5]. Such complex exploits may not seek immediate gain, instead attempting to acquire covert access over a lengthy period to extract confidential and critical data necessary to achieve the attackers' aims [6]. The incursion of APTs can lead to numerous detrimental organizational consequences, including intellectual property theft, data breaches, critical infrastructure disruption, and potentially complete takeovers of the affected site [7]. Furthermore, governments have regularly supported APT attacks and utilized them as cyber warfare by exploiting vulnerabilities [8]. Smartphone mobile security challenges have emerged due to its pervasive adoption and rapid mobile hardware and software technology advancements. An ongoing concern regarding smartphones is their susceptibility to being the primary target for APT attacks. Most mobile APTs depend on social engineering assaults through sensors, including spear phishing, application repackaging, watering holes, and SQL injection.

Several vulnerabilities lead to APTs, such as heterogeneous mobile network protocols, physical mobile devices, sensors, applications, and services. For instance, smartphones are vulnerable to APT attacks due to insecure communication protocols in mobile networks such as Wi-Fi and Bluetooth. These unencrypted communication protocols make it easier for attackers to intercept and eavesdrop on the communication between devices. In addition, many mobile devices lack built-in security measures such as firewalls, encryption, and intrusion detection systems, leaving them vulnerable to Wi-Fi and Bluetooth attacks and other types of APT attack. Additionally, attackers can use social engineering tactics, such as phishing, to trick users into revealing sensitive information or downloading malicious software [9,10].

Smartphone sensors are essential for gathering, transmitting, and analyzing information in a smartphone application. A smartphone has several sensors and services critical to the user's everyday activities and potentially includes sensitive data. The vulnerabilities in mobile sensors include limited capacity, low-cost sensors, and their nature of always being "ON" [11]. These conditions may lead to increased attack surface as mobile devices' increased connectivity and availability increase their susceptibility to attacks. Sensors can gather sensitive information, such as location and biometric data, which can be used in further attacks. Furthermore, mobile devices can easily spread malware to other devices in the network, as they are often used to access sensitive information and connect to other networks. Thus, financial and privacy loss and reputational damage are the main impacts that can harm the systems of individuals and organizations. Thus, smartphones have become the principal target of attackers undertaking APT assaults [12] including AndroRat [13], FinSpy [14], and Asacub [15].

Extensive use of third-party mobile application stores and the risk of lost or stolen smartphones add to the potential vulnerabilities, making them more susceptible to APT attacks. Due to the stealth, flexibility, and persistence of APTs, detecting such attacks using existing strategies, such as network monitoring and analysis, endpoint detection and response, user behavior analysis, and data loss prevention (DLP) technologies, can be challenging. Various security technologies are available to detect and prevent the exfiltration of sensitive data from an organization, a common objective of APT attacks [16,17]. In order to penetrate the system, hackers use social engineering methods, zero-day vulnerabilities, and long-term latent approaches [18]. Ultimately, high-level security networks are becoming increasingly vulnerable to this threat [19].

Various vulnerabilities in smartphones lead to APTs. For instance, the large surface of attack occurs due to heterogeneous mobile network protocols (Wi-Fi, SMS, GPS, email, web) and vulnerabilities in smartphone sensors as a result of sensor data being accessible by default and having no permissions [20,21]. Consequently, APT is deemed as a highly sophisticated variant of multistep assault [22]. Given their sophisticated methodologies and usage of previously undisclosed vulnerabilities, APTs pose a challenge to current detection tools.

The economic costs of a successful APT attack can be tremendous, and investments in intrusion detection and prevention systems are often motivated by the potential costs of such attacks [23]. A broad range of cyber threats, such as malware and suspicious activity that potentially leads to phishing attacks, may be detected using AI, which can analyze millions of datasets in minutes. As new forms of assaults are discovered through AI application, it is constantly refined and enhanced [24,25].

Despite studies having been undertaken and several APT solutions developed and implemented, none has offered a comprehensive solution. The reason is due to several challenges and limitations. Firstly, there is insufficient fingerprinting of APT attacks. Fingerprinting of attacks uses sequential tactics, techniques, and procedures (TTPs). Due to difficulties in detecting an APT assault, attackers may utilize various strategies and approaches to launching it. User behavior for tackling APT has never been conceptualized and comprehended. Thus, user actions for handling smartphones while using mobile applications, completing job-related tasks, the environment and surrounding contextual parameters, user intentions, and device permission have not been clearly and precisely defined. With no data on normal user behavior, there is no distinction between APT security attacks [26]. The second limitation is the issue of characterizing the interconnected attack routes formed by APT attackers when they exploit vulnerabilities [27]. Due to the dynamic APT attack process, this form of attack is constantly evolving. The success of an APT attack can be influenced by two factors: how the attack is carried out and when it is launched.

Similarly, the security approaches implemented for personal computers, such as desktops and laptops, may also be performed for mobile devices, such as smartphones. On the other hand, cell phones have a few distinguishing characteristics that lead to significant issues with ensuring their security [28]. For example, products designed for the general public, such as smartphones, are typically open platform systems with multiple entry points and central data management, making them vulnerable to theft and loss. Additionally, embedded sensors and limited battery life can further increase their security risks [29].

In addition, the behavior of granting permissions requested by applications is observed as a user behavior that contributes to cyber attacks. Based on the challenges mentioned in detecting APTs, a comprehensive systematic survey was conducted in this study. A total of 1351 papers analyzed from the past ten years (2012 to 2023) were analyzed. The primary aim of the conducted systematic literature review (SLR) is to understand and analyze existing studies and present concrete findings by detecting APT on mobile sensors, applications, and services. Subsequently, a conceptual framework was also proposed for the situational awareness model in line with adopting game theory as an AI technique.

The cyber cognitive situational awareness (CCSA) model was explored, and its suitability to detect APT attacks on smartphones was tested. The study aims to fulfill the following research objectives: (i) to conduct a comprehensive SLR concerning APTs on mobile sensors with game theory as an AI technique. (ii) To provide a concrete discussion and analysis of findings for the SLR and generate recommendations on detection. (iii) To analyze the open challenges of APTs on mobile sensors, applications, and user behavior. (iv) To propose a conceptual model and an open discussion to identify solutions for APTs on smartphone sensors.

This study provides an SLR of APT detection for mobile devices and an exploration of AI techniques, such as game theory, as a potential solution. It can be used to design guidelines and policies to secure against APT attacks on mobiles and raise awareness of the challenges, effects, and consequences of APT attacks. It has identified, explored, and evaluated various detection mechanisms used to detect APTs on smartphones and proposed a conceptual framework for the situational awareness model. Finally, the review and proposed conceptual framework (FORMAP) have addressed the gaps concerning the detection of APTs in smartphone sensors, applications, and behavior. Figure 1 illustrates the outline structure of this research study.

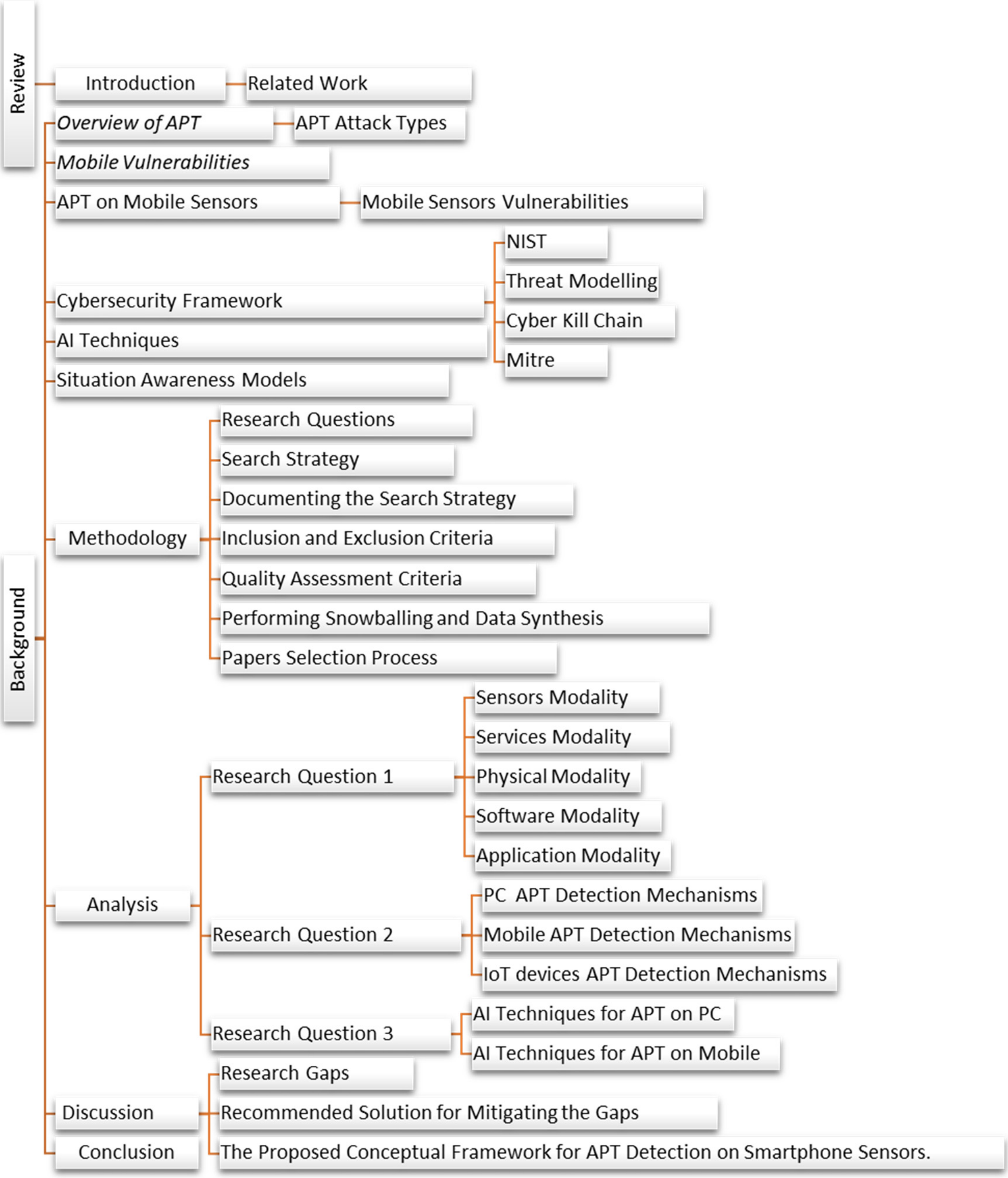
Review
Introduction
Related Work
Overview of APT
APT Attack Types
Mobile Vulnerabilities
APT on Mobile Sensors
Mobile Sensors Vulnerabilities
NIST
Threat Modelling
Cybersecurity Framework
Cyber Kill Chain
AI Techniques
Mitre
Situation Awareness Models
Research Questions
Search Strategy
Documenting the Search Strategy
Methodology
Inclusion and Exclusion Criteria
Quality Assessment Criteria
Background
Performing Snowballing and Data Synthesis
Papers Selection Process
Sensors Modality
Services Modality
Research Question 1
Physical Modality
Software Modality
Application Modality
PC APT Detection Mechanisms
Analysis
Research Question 2
Mobile APT Detection Mechanisms
IoT devices APT Detection Mechanisms
AI Techniques for APT on PC
Research Question 3
AI Techniques for APT on Mobile
Research Gaps
Discussion
Recommended Solution for Mitigating the Gaps
Conclusion
The Proposed Conceptual Framework for APT Detection on Smartphone Sensors.

Figure 1. The Outline Structure.

The remainder of this paper is structured as follows. After this introductory section, the background of APTs on smartphone sensors is introduced in Section 2. The SLR protocol and the relevant steps are presented in Section 3. Subsequently, Section 4 focuses on the SLR analysis of the selected studies to respond to the formulated research questions. Finally, the discussion, recommendations, limitations, and conclusion are outlined in Sections 5 and 6, respectively.

Related Work

The detection of APTs has challenged current defense systems in cyber security. Different SLRs and review articles have been undertaken to discuss and analyze the detection of APTs. Recent models have been developed and significantly contributed to the cyber security field to help understand the behavior of APT attacks. Table 1 presents previous review studies.

Table 1. Previous SLR Studies.

SLR	Year	Type	Period	Techniques	NIST	Framework	Review Focus
[30]	2023	Systematic	2017–2023	Game theory	Detection	No	Game theory approaches and strategies utilized to optimize the defensive performance of security measures
[31]	2023	Narrative	-	Deep learning	Detection	No	Detection of malware using deep learning techniques on Android, iOS, IoT, Windows, APT
[32]	2022	Systematic	2011–2022	Risk and trust	Identification	Yes	Various defense mechanisms to protect against APTs, including advanced approaches
[33]	2022	Systematic		AI algorithms used to detect beaconing behavior	Detection	No	Various APT-specific detection techniques and solutions by focusing on detecting C&C malware
[34]	2022	Narrative	-	Intelligent threat profiling	Identification/Detection	Yes	Highlighting intelligent threat profiling's multisource data, important approaches, and common applications
[35]	2022	Narrative	-	-	-	No	Provided a comprehensive overview of APTs and information on how APTs work in classifying defensive techniques, which have included monitoring, detection, and mitigation
[36]	2021	Narrative	-	Threat modeling	Identification	No	Identifying any possible enhancements that may improve threat modeling performance
[37]	2021	Narrative	2010–2020	Unsupervised Louvain algorithm	-	No	Investigation of bibliometric indicators to provide generic research themes and aggregated communities
[38]	2021	Systematic	-	Game theory	-	No	Application- and metric-based categorization that balances security, cost, and usefulness
[39]	2020	Systematic	2011–2017	Analyzing previous APT detection mechanism	Protection/Detection	No	Analyzing a few defense frameworks for detection and prevention of APT
This study	2023	Systematic	2012–2023	Game theory	Detection	Yes	Detection of APT on mobile devices based on applications and sensors

For instance, Khalid et al. [30] studied and analyzed the research articles published in various journals between 2017 and 2022. The studies utilized game theory to deal with APT attacks. According to the study, game theory proves to be a valuable tool in examining the dynamics of the interactions between attackers and defenders. It has been used to enhance security measures, prepare for countermeasures, and design contracts that benefit both parties.

Furthermore, game theory has been applied to enhance the security of diverse systems, such as cyber-physical systems, social networks, and transportation systems. It is evident that game theory is a useful tool for analyzing and comprehending complex security situations in the face of technological advancements, evolving threat landscapes, and new trends in cyber crime. It is concluded that although APT attacks are expected to become increasingly sophisticated and evolve over time, game theory will remain a crucial tool for addressing them.

Moreover, a detailed survey of [31] focused on recent advancements in deep learning-based malware detection techniques, tracing the evolution from traditional approaches. The study examined sandboxing methods, deep learning models, and the detection of emerging malware types, including ransomware and APTs, as well as traditional malware affecting IoT, Windows, Android, and iOS platforms.

In contrast, Thulfiqar et al. [32] studied and analyzed various defense mechanisms deployed to counter APTs on both networks and devices. In addition, the review has concentrated on and provided a detailed analysis of the risk management strategies used to detect APTs. The authors proposed the utilization of the observe–orient–decide–act (OODA) model as a means of generating mobile device behavior fingerprints for the purpose of defending against APTs. The model monitors device behavior to detect suspicious behavior in all stages of the APT lifecycle.

The authors of [33] discussed the strategies and procedures that can be utilized to identify APTs, specifically to recognize beaconing, during the lifecycle of an APT.

Many different AI algorithms have been determined to identify, analyze, and compare the characteristics of datasets and data sources used to put these detection techniques into action. In addition, the benefits and difficulties associated with many different APT beaconing detection techniques have been discussed. This SLR offered a broad overview of APT attack detection in smartphone sensors, applications, and services. It revised 96 papers on APTs in smartphones during the last decade.

In addition, a comprehensive analysis [34] was conducted to investigate intelligent threat profiling strategies designed specifically for APTs. The evaluation focused on a wide range of topics, such as data processing, threat modeling, representation, and reasoning methods. The research highlighted the significance of threat profiling in developing an intelligent security ecosystem by presenting a framework for intelligent threat profiling to enable proactive defense against APTs. The research addressed the challenges associated with APT defense and offered technical assistance in developing an intelligent platform. These challenges were addressed through the utilization of knowledge graph and deep learning techniques.

Khaleefa and Abdulah [35] presented a comprehensive analysis of APT implementation, covering various aspects such as definitions, methodologies, and the classification of defensive measures, including monitoring, detection, and mitigation. The technical underpinnings of extant APT detection and mitigation protocols, as well as the evaluation criteria for efficacious defensive tactics, pivotal datasets, and the present state of advancement in the domain, were also deliberated upon by the participants.

Meanwhile, Tatam et al. [36] discussed potential enhancements in threat modeling approaches to effectively address sophisticated attacks, including APTs. They emphasized the necessity of employing a hybrid approach that combines various methods due to the intricate nature of existing systems. The authors also emphasized the importance of maintaining threat visibility at all phases and levels, while acknowledging that no specific threat-modeling method can encompass all possible situations.

In a bibliometric analysis performed by Bhat and Kumar [37] on articles related to APTs, they identified common research themes and closely linked communities based on indicators such as co-authorship, citations, and publication forums. Their multidisciplinary perspective provided valuable insights into the current trends in APT research.

Kumar et al. [38] conducted a comprehensive assessment of game theory strategies categorized as application-based and metric-based classifications to facilitate impartial decision making concerning countermeasures against APTs. The aforementioned factors, namely security, cost, and usability, were taken into account. The investigation has revealed that there are certain limitations associated with the application of game theory. The limitations of game theory encompass the dependence on presumptions regarding the conduct of the involved parties, alongside the challenges linked to scrutinizing intricate games that involve numerous participants. The research yielded valuable perspectives on APT behavior, streamlined the decision-making process for optimal resource allocation, and emphasized the importance of incorporating practitioner viewpoints to enhance information security risk management.

Finally, Hussain et al. [39] thoroughly analyzed APTs and the communication method that connects a compromised system to a command-and-control (C&C) server. It is the location where persistent malware receives commands and captured data are exfiltrated. In addition, the authors suggested conducting research on an APT defensive framework for industrial control systems and presenting their findings. During the C&C phase of the APT lifecycle, this framework provides a layered security and detection solution for the organization network that is different from the current review as it sheds light on the detection of APTs on smartphones. Nevertheless, the review does not include APT detection techniques for mobiles and situational awareness models while missing a game theory-based approach.

2. Background

Section 2 emphasizes the importance of understanding APT attacks thoroughly and techniques involving AI. This understanding is essential for appreciating the SLR conducted. Thus, this section provides an overview of APTs, threat modeling, MITRE attack framework, and AI.

2.1. Overview of Advanced Persistent Threats (APTs)

The targeted attack strategy used by a qualified and skilled adversary to maintain undetected access to critical information exfiltration for a lengthy period is known as an APT. There are various forms of APT assaults, including social engineering techniques such as spear phishing, SQL injection, malware, and watering hole attacks [3]. The term APT offers shorthand for what it is. Traditional assaults lack one or more of these traits.

"Advanced" means the attacks are planned by a team of individuals with many resources, expertise, and funding. The assaults must be simple to be successful. It is common for an attacker to utilize phishing and readily available malware development tools [40,41]. Nevertheless, when necessary, they utilize software, such as zero-day exploits, to target particular vulnerabilities and launch several attacks to gain access. "Persistent" attackers are desperate to access the victim's systems, applications, and resources. Resultantly, the intruder has full access to the system, including backdoors. If one connection is compromised, others may be opened and used to continue collecting sensitive information. Distinguishing between a threat and an opportunity is also important. Since they are more than software that runs independently, APTs pose a problem [12,42,43].

There are two types of APTs, namely killing and leeching. Leeching occurs when an attacker passively gathers information from a target system without compromising it. An attacker may use a network sniffer to steal sensitive data. Leeching is a sneaky attack that gives attackers information they can use to launch more serious attacks. On the other hand, killing involves actively compromising and disrupting a target system.

Malware can compromise a system, delete important files, or steal sensitive data. Killing is a more aggressive attack that can damage a target system and is easier to detect than leeching [44]. The primary difference between leeching and killing is the attacker's intent. Leeching is typically motivated by the desire to gain access to information or resources, while killing is motivated by the desire to disrupt or destroy systems and networks. Thus, the tactics used to defend against leeching and killing are different. Preventing unauthorized access is the focus of defending against leeching, while protecting against disruptions is the focus of defending against killing [44].

2.1.1. APT Security Attack Types Penetrating Mobile Phones

Most mobile APTs depend on social engineering assaults through sensors, including spear phishing, application repackaging, watering holes, and SQL injection [45]. Based on the target, an APT attack may utilize a combination of different attack vectors, as indicated below (see Figure 2):

- Social engineering: Obtaining a user's assistance in compromising information systems. This approach manipulates individuals with privileged access into disclosing personal information to carry out a harmful attack through control and persuasion [46].
- Spear phishing: This approach usually obtains user credentials, financial details, or private information from a single business [47].
- Watering hole: It is similar to spear phishing in terms of cyber espionage. The attacks are adjusted to the victims' needs. Additionally, it attempts to acquire information regarding victims based on their particular interests [48].
- Application repackaging: Application repackaging creates a new version of an existing software application, often to modify its functionality, compatibility, or distribution method. This process typically involves decompiling the original application, modifying its code and resources, and subsequently recompiling it into a new package [49,50].
- Malware: It has become one of the biggest threats to corporations and organizations that practice bring your own device (BYOD). Various attacking vectors are available for malware to transmit and release their payload, especially in BYOD environments [45].

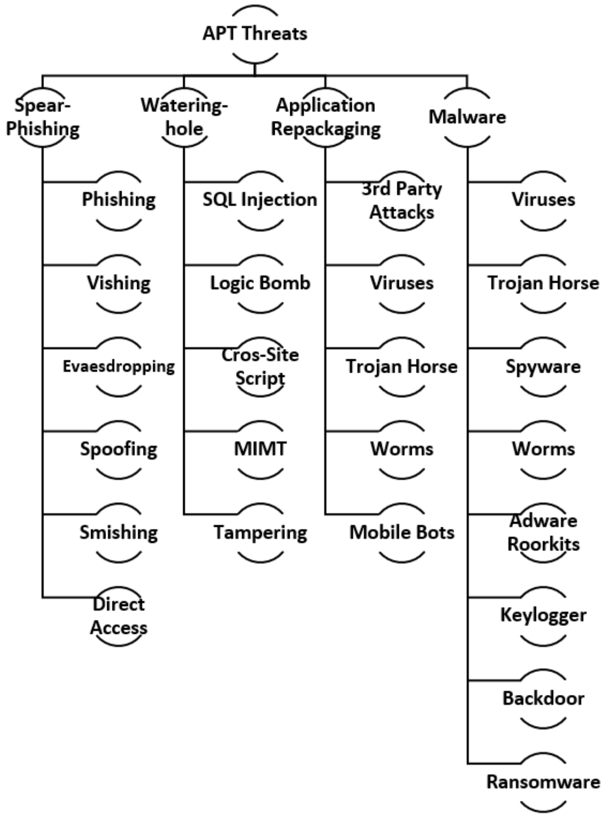

Figure 2. APTs and Their Attacks.

2.1.2. APT Attack Lifecycle and Its Impact

As seen in Figure 3, the APT attack lifecycle includes the following eight stages:

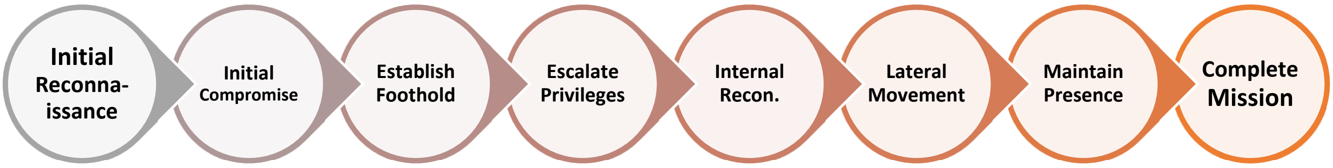

Figure 3. The APT Lifecycle [51].

Stage 1: Conducting a survey is the initial step towards launching a targeted attack. The research and information regarding the targeted organization are acquired to break the organization's border security.

Stage 2: Comprises employing various entry vectors to obtain the first footing within a network.

Stage 3: On the server or endpoint, malicious code is run, granting complete control of the computer or system. This stage will develop a strong attempt to retain persistence beyond the first agreement.

Stage 4: After gaining complete control of the compromised node, attackers will try to acquire additional access to the system and data by targeting privileged accounts.

Stage 5: The attacker is attempting to gain recognition once again through the internal network. Various methods, such as searching for files and directories, are utilized to locate valuable targets.

Stage 6: These techniques can be used by an intruder to gain unauthorized access and make modifications to internal network systems.

Stage 7: The APT utilizes malware backdoors or a remote administration tool to maintain a foothold in the network's environment.

Stage 8: Before data exfiltration, the attacker must retrieve private data from remote devices [11].

As stated earlier, APT refers to an intrusion activity in which an attacker establishes an illegal, long-term presence on a network to capture sensitive data [8]. Cyber attacks using APTs are frequently targeted towards large organizations or government networks. Such intrusions have a plethora of consequences, including intellectual property theft, sensitive data breach, critical company infrastructure disruption, and entire site takeovers. Additionally, government-sponsored APT assaults are frequently utilized as cyber warfare weapons.

2.2. Mobile Vulnerabilities

Smartphones have become an integral part of people's daily lives and play a major role in personal and professional aspects. Nevertheless, their widespread use and the sensitive information stored make smartphones an attractive target for cyber criminals. Resultantly, understanding the vulnerabilities that exist in these devices is vital. As viewed in Figure 4, some common vulnerabilities in smartphones include physical factors and lost or stolen devices. Moreover, mobile services often have default settings allowing users to download and install applications without properly scrutinizing the potential risks involved. One of the sensors, such as a camera or microphone, might be unexpectedly turned on by default. Allowing numerous permissions and accessing this permission can damage the system and data and lead to escalating privilege.

Employing mobile security reference architecture (MSRA) alone is insufficient as attacks evolve from time to time, leading to the inability to tackle the attack and difficulties in recognizing new attacks [2]. In addition, large attack surfaces are due to various mobile network protocols (Wi-Fi, GPS, short messaging services (SMSs), multimedia messaging services (MMSs)). Mobile sensors are vulnerable to unauthorized access due to default settings that allow access to sensor data without permission. The small size and low cost of these sensors, and their default "always ON" mode, increase the likelihood of potential attacks.

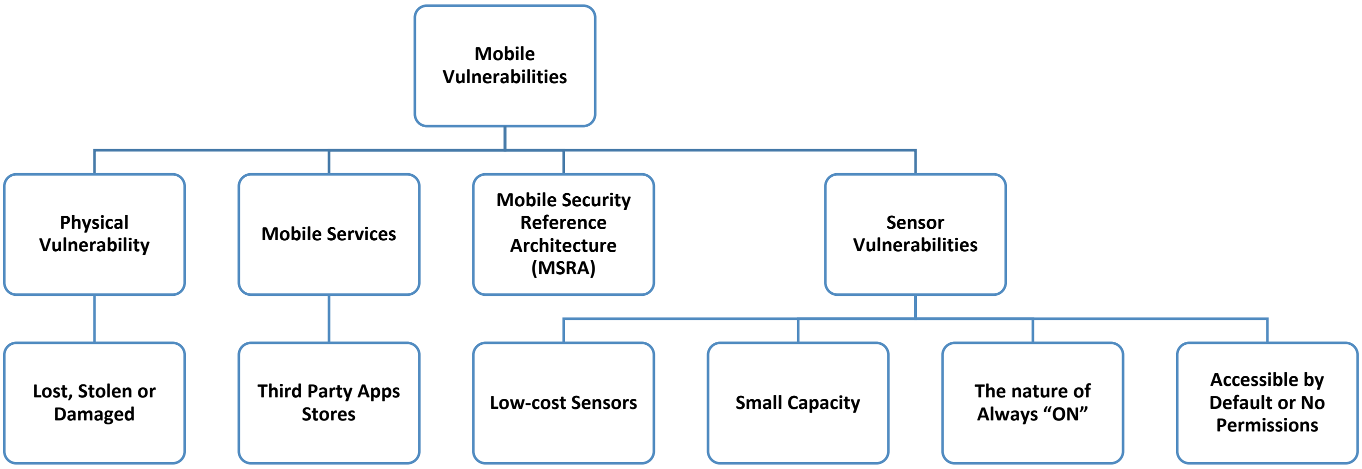

Figure 4. Mobile Vulnerabilities.

2.3. Overview of APT Attacks on Mobile Sensors

Mobile sensors are classified into three types [52]: inertial, positioning, and ambient. Figure 5 illustrates the classification of smartphone sensors. Inertial sensors on a smartphone are required to control the orientation of the user interface and detect events. Accelerometer and gyroscope sensors can be used to detect events such as device management, tilting, and dropping. Positioning sensors, such as global positioning systems (GPSs) and Wi-Fi, are essential for specifying the location of devices and transmitting information. Additionally, ambient sensors, such as microphones and cameras, must detect and analyze the user's environment, share documents, and interact with other Internet of Things (IoT) devices that utilize the same technology.

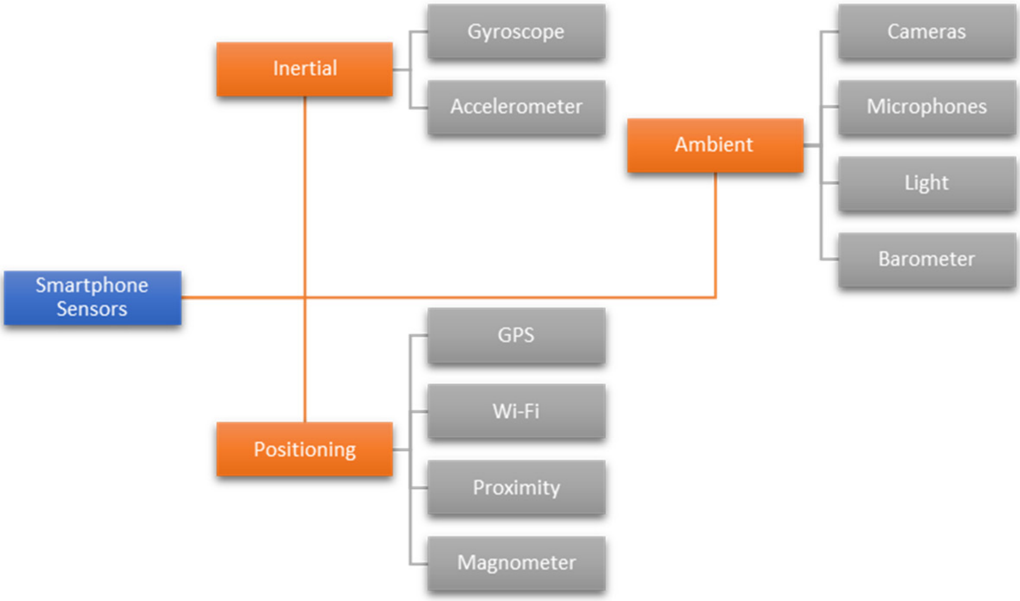

Figure 5. Smartphone Sensor Classifications [12,14].

SMS, MMS, and other telecommunication services such as calls, phone logs, and other services, including the calendar, create a constant data stream. As a result, sensor access is required for various services. Once an attacker obtains or reads these data, the user's protection may be threatened. These features depend on the user's attention [53], and the perpetrator has the ability to execute a highly active APT attack on the mobile to exploit this dependency [12].

Regarding to Zulkifli et al. [53], social engineering can facilitate file transmission and sharing. Among such sensors are Bluetooth connection and the Android beam. The malware also compromises APT target location, environmental sensors, and sensitive data resources. Thus, an APT assault on a mobile phone is a plausible scenario. The Baumgartner et al. [54] assault used an attachment in a spear-phishing email to target a Tibetan activist.

The GPS and Wi-Fi sensors can be compromised due to a flaw. Androrat [13] used application repackaging to target cellphones' GPS, Wi-Fi, camera, and microphone sensors in an assault that affected Turkey and the United States (US). Finally, an assault targeted Bahraini human rights advocates [14] using spear-phishing emails that exploit GPS, Wi-Fi, Bluetooth, and microphone sensors [12].

Vulnerabilities of Smartphone Sensors

Due to the vulnerabilities, an attacker can use smartphone sensors and initiate an APT attack. Vulnerability analysis of sensors discovers and prioritizes these flaws as part of developing security policies and procedures. According to Table 2, several vulnerability spots exist in smartphone sensors, resulting in several cyber attacks launched to take advantage of the vulnerabilities in smartphone sensors. For instance, MIMT and reply attacks can be carried out using communication channel gaps in GPS sensors. The Bluetooth sensor has various vulnerabilities, including LMP/LLP.

Exploiting this vulnerability may allow for executing variant attacks such as hijacking, blue sniffing, or sniffing. Additionally, near-field communication (NFC) sensors are vulnerable to attacks such as eavesdropping and spoofing due to a lack of communication security. Lastly, the vulnerabilities of the camera and microphone sensor have resulted in various security risks, including side-channel attacks and eavesdropping. A strong understanding of the sensors and their vulnerabilities helps designers and users of security systems avoid being targeted.

2.4. Cyber Security Framework in Organizations

The framework integrates industry standards and best practices that assist companies in managing risks associated with cyber security. It provides a standard vocabulary that enables personnel at all organizational levels and supply chain nodes to build a shared awareness of their cyber security threats. Since its publication in early 2014, the framework has been used as a guide by both the corporate and public sectors. Due to the successful effort, Congress made it a duty of the National Institute of Standards and Technology (NIST) in the Cybersecurity Enhancement Act of 2014 [55].

2.4.1. NIST Cybersecurity Framework

The National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity provides a framework for measuring and enhancing private sector businesses' capabilities to prevent, detect, and respond to cyber events [56]. The US NIST issued Version 1.1 in April 2018, and has received rapid acceptance across various sectors. The framework guides cyber security operations by utilizing business drivers and regards cyber security as a component of an organization's risk management procedures. Numerous firms have used this paradigm to assist them in managing their cyber security risks [56,57]. The five core functions (identify, protect, detect, respond, and recover) of NIST offer a holistic perspective of an organization's cyber security risk management lifecycle and should be used as a reference point [57].

Table 2. Loopholes of Mobile Sensors.

Sensors	Vulnerability	Security Threats/Attacks
GPS [58]	Unsecure channel	MIMT/Replay attack
	Lack of permission	Privacy attack
Bluetooth [59]	Vulnerability in LMP/LLP	Hijacking attacks/blue sniffing or snigging attacks
	A cheap antenna can increase the attack distance	Range extension attack
Gyroscope and accelerometer [60]	Have no access control mechanism/Permissions	Side-channel attacks, tap logger attacks, tap prints attacks, eavesdropping attacks
Gyroscope, accelerometer, and magnetometer [61]	Lack of fingerprinting technique	Sensor ID attacks
NFC [62]	Unsecure communication	Eavesdropping attacks
	URL/URI deceiving	Spoofing attack
	Unauthenticated NFC device	Tag replacement and tag hiding (TRTH) attack
Microphone [61,63,64]	Unsecure environment	Eavesdropping attacks
	Unsecure smartphone password	Acoustic side-channel attack
Camera and microphone [61,63,64]	The preinstalled camera app might grant other apps, camera, and microphone access	Eavesdropping attacks and spyware
	Without users' consent, photos and videos can be taken	Eavesdropping attacks and spyware
	Lack of privacy, location can be tracked	Privacy attack

2.4.2. Definition of Threat Modeling

Threat modeling is a technique for systematically identifying potential security vulnerabilities and associated dangers. It serves as a framework for evaluating controls, protecting devices, and plays a critical role in creating safe applications [43]. Additionally, threat modeling develops and formalizes a methodology for risk assessment and vulnerability analysis of a single or group of information and communication technology (ICT) assets [65]. It aims to proactively identify, categorize, and characterize risks associated with an attack on the camp.

To recognize attackers' behavior in a network, visibility of odd actions or behavior discovered by indicators is required. Numerous threat-modeling techniques have been created, including STRIDE, attack trees, kill chain, ATT&CK, diamond, and TARA. These techniques can be combined to create a more complete and accurate picture of potential threats [36].

2.4.3. Cyber Kill Chain

Lockheed Martin first released the cyber kill chain framework as part of the Intelligence Driven Defense model for identifying and preventing cyber incursions [66]. The model specifies the steps adversaries must take to accomplish their aim, including network targeting, data exfiltration, and persistence within the business.

This model demonstrates that disrupting adversaries at any point in the chain of assault breaks the attack chain [67]. The cyber kill chain concept generally comprises seven phases: (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control, and (7) objective-related actions [68]. These phases give information on the attacker's TTPs.

2.4.4. The Framework for Attacks (MITRE)

The acronym MITRE denotes the Massachusetts Institute of Technology's Center for Research and Engineering, Adversarial Tactics Techniques, and Common Knowledge [36]. The MITRE attack methodology provides a comprehensive overview of how cyberattackers gain entry into networks, navigate laterally, elevate access privileges, and circumvent security measures, all within a single resource [69]. This approach is employed by cyber security researchers to identify and classify cyber attacks and assess the risk to the organization. The assumptions of MITRE ATT&CK are analogous to those of other cyber security frameworks.

In contrast to other cyber security solutions, MITRE ATT&CK operates under the assumption that a breach will inevitably occur and adopts an attacker-centric approach to address this issue [70]. Twelve potential tactics or objectives of an attacker are outlined, which include initial entry, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact [71]. Additionally, numerous attacking techniques, such as drive-by compromise, spear phishing, and rootkit attacks are mentioned [36,72].

2.5. AI Techniques in Detecting APT Attack

Artificial intelligence (AI) is a subfield of computer science that enables robots to think and act like humans. It uses machine learning, deep learning, optimization, game theory, and evolutionary algorithms. Machine learning is predicated on the assumption that a machine can learn by identifying patterns in given data and make accurate decisions with little human intervention [73].

Due to the nature of APTs, detecting and preventing them can be a significant challenge. Nevertheless, various AI techniques can help detect APTs and mitigate the damage they cause. Some of the most commonly used AI techniques for detecting APTs are machine learning, deep learning, fuzzy logic, and game theory. These AI techniques have been used to solve problems and increase efficiency in detecting smartphone APT attacks [74].

In addition, adopting AI to detect APTs has many advantages. Firstly, it is difficult for individual analysts to process and detect threats in time due to the enormous amount of information generated by APT attacks. However, AI methods can process massive amounts of data rapidly and accurately, accelerating the detection of APT attacks. Due to their complexity and stealthy nature, traditional security measures often fail to identify APT attacks.

Nonetheless, AI techniques can examine sophisticated behaviors and spot deviations that might indicate an APT. As APT attacks can persist for weeks or months, continuously monitoring the networks is crucial. Such monitoring can be undertaken with the help of AI techniques, lowering the possibility of an APT attack going undetected. The number of false positives in APT detection can be decreased with the assistance of AI techniques. Lastly, APT attackers are constantly modifying their methods. Hence, security measures must be flexible enough to keep up with the attacks. Therefore, modern APT attacks can be detected by AI algorithms as they learn from new data and refine their models [75].

2.6. Situation Awareness Models

Situation awareness models refer to systems or models designed to provide an understanding of the current situation, including the state of the environment, current objectives, and actions taken. These models aim to provide a comprehensive, real-time picture of a situation to ensure that individuals or systems can make informed decisions. According to Endsley's well-accepted situation awareness model [76,77], there are three levels of situation awareness perception, integration and comprehension, and prediction. In the first level, situation awareness encompasses the critical information observation concept. The second level involves the integration and interpretation of essential information. In the third level, the situation awareness model is concerned with the awareness to predict possible environmental events [78].

Several situation awareness models exist, including cognitive, decision-making, and information fusion models. Cognitive models focus on the mental processes of situation awareness, such as perception, attention, and memory. On the other hand, decision-making models focus on the processes involved in using situation awareness information to make decisions. Information fusion models combine information from multiple sources to provide a complete situation picture. The situation awareness models are used in various fields, including the military, aviation, healthcare, and transportation [77,79].

Section 3 discusses the research methodology implemented to carry out the research for discussion and analysis.

3. Research Methodology

This systematic literature review (SLR) was conducted to comprehensively and precisely address the specific concerns as formulated in the research questions. A comprehensive analysis was performed using the gathered research data, and the most notable studies pertaining to the identified issues were documented.

The main objective of this SLR is to collect the most pertinent articles from primary sources. The papers underwent analysis and assessment to ensure the attainment of precise findings, as the principal objective of an SLR is to establish unbiased methodology [80,81]. Similar attempts have been made to minimize biases to achieve the objectives. The SLR design is composed of several phases, as illustrated in Figure 6. The SLR methodology entails a series of sequential processes, which include the identification of research questions, development of a search strategy, documentation and execution of the search strategy, selection of studies based on inclusion and exclusion criteria, evaluation of quality criteria, and quantitative meta-data analysis. The subsequent section provides a detailed explanation of all the aforementioned stages.

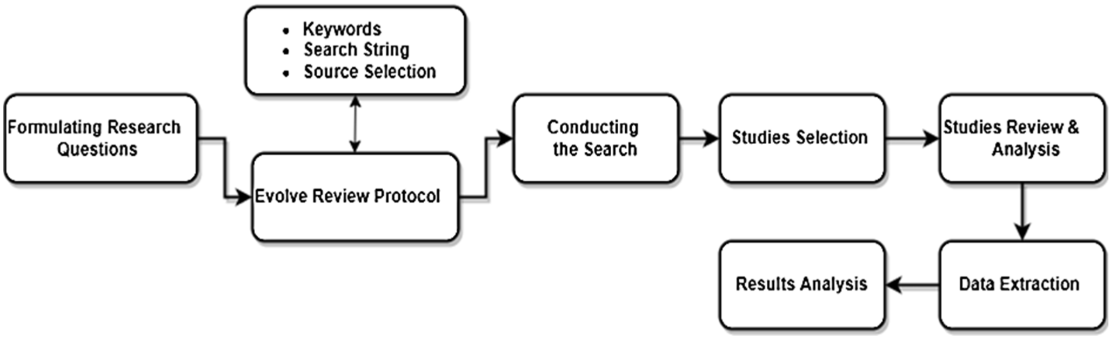

Figure 6. Methodology to Design SLR.

3.1. Research Questions

The primary objective of this SLR is to formulate security-related questions and offer clear solutions to those concerns. The research questions provide the foundation for discussing APT detection for smartphone sensors and applications. Based on the collected studies, three research questions were established and answered in this research study. Table 3 contains the motivations for and a detailed description of these questions.

Table 3. Research Questions.

Research Question	Description and Motivation
(RQ1) What activity is carried out by a user on a smartphone that is highly vulnerable to a security attack?	The question aims to shed light on user activities and behaviors the attacker could exploit to compromise the smartphone through its sensors.
(RQ2) What are the detection mechanisms of APT attacks on a mobile phone?	RQ2 is motivated by the need to identify the mechanisms utilized to detect APT attacks on a smartphone.
(RQ3) What challenges and problems might appear in adopting AI techniques for detecting APTs in mobile sensors?	The motivation for RQ3 is to address the problems and challenges of existing studies on adopting AI techniques to detect APTs on smartphone sensors.

3.2. The Search Strategy

As the search strategy is critical to any research, the emphasis was on properly organizing the search approach. In this level of the SLR protocol, the first step was to create a search string from the keywords. Finding articles requires more than only keywords. The keywords must be combined in several ways to form a string acceptable for various publications and digital libraries [82,83]. The search strategy was categorized into four stages: keyword definition, search string construction, source selection, and search technique.

3.2.1. Defining Keywords

To ensure the acquisition of the most pertinent outcomes from articles, specific keywords were designated for each individual inquiry. Table 4 presents a comprehensive inventory of the established terms utilized for the purpose of conducting searches. The primary topic's keyword search was formulated by combining the keywords extracted from each question. The following keywords were also used in the search to have the most relevant information on the subject.

Table 4. The Keywords of The Research Questions.

Research Questions	Keywords
(RQ1) What activity is carried out by a user on a smartphone that is highly vulnerable to a security attack?	("user activity*" OR "user behavior*" OR "user interaction*") AND ("Mobile*" OR "smartphone*") AND ("vulnerability*" OR "loophole*") AND ("security*")
(RQ2) What are the detection mechanisms of APT attacks on mobile phones?	("Mobile*" OR "smartphone*") AND ("APT threat*" OR "advanced persistent threat*" OR "APT attack*" OR "cybersecurity attack*") AND ("detection*")
(RQ3) What challenges and problems might appear in adopting AI techniques for detecting APTs in mobile sensors?	("artificial intelligence*" OR "AI*" OR "fuzzy*" OR "game*") AND ("Mobile*" OR "smartphone*") AND ("APT*" OR "advanced persistent threat*" OR "cyber*" OR "threat*" OR "attack*") AND ("detection*") AND ("game theory*")

3.2.2. Forming Search String

A search string was constructed using the keywords associated with a specific question. The search string was confirmed by security and mobile networking specialists. The search string was validated against the sources and adjusted to obtain the most relevant results. The following stages were followed to create the search string [84].

(1) Major words were derived from the topic and research questions.

(2) Identifying other spellings or alternatives for significant phrases.

(3) Identifications of keywords.

(4) The Boolean operator "OR" indicates synonyms or other spellings.

(5) The following search string was formed based on the above operation.

("activity*" OR "behavior*" OR "interaction*") AND ("Mobile*" OR "smartphone*") AND ("vulnerability*" OR "loophole*") AND ("security*") AND ("APT threat*" OR "advanced persistent threat*") AND ("detection*") AND ("artificial intelligence*" OR "AI*") AND ("game theory*").

Pilot searches were undertaken to improve the quality of the results and the search. The search string is divided into two sections. The first section focuses on APTs targeting smartphones, while the second section explains the AI algorithms used to detect APTs.

3.2.3. Selection of Database Sources

For data collection, several libraries and databases were consulted. These sources are the most relevant libraries, covering several aspects of the subject under discussion, such as computer sciences, information technology, risk assessment, and network security. These databases provide a large variety of peer-reviewed research articles relevant to the fields of AI, human–computer interactions, cyber security, and mobile computing. In addition, these libraries comprise easy-to-use, powerful search engines better suited for automated searches [85]. Table 5 contains the list of these libraries and their websites.

Table 5. The Database Sources.

Database Source	Website
ACM	dl.acm.org recent access 8 June 2023.
IEEE	ieeexplore.ieee.org recent access 8 June 2023.
ScienceDirect	www.sciencedirect.com recent access 8 June 2023.
Scopus	www.scopus.com recent access 8 June 2023.
Springer	link.springer.com recent access 8 June 2023.

3.2.4. Search Process

The search process focused on studies published between 2012 and 2023. Automatic and manual searches were undertaken to locate relevant initial studies. A manual search was conducted to verify the search string. Figure 7 presents the number of studies for all research questions that have been retrieved from the online databases resources.

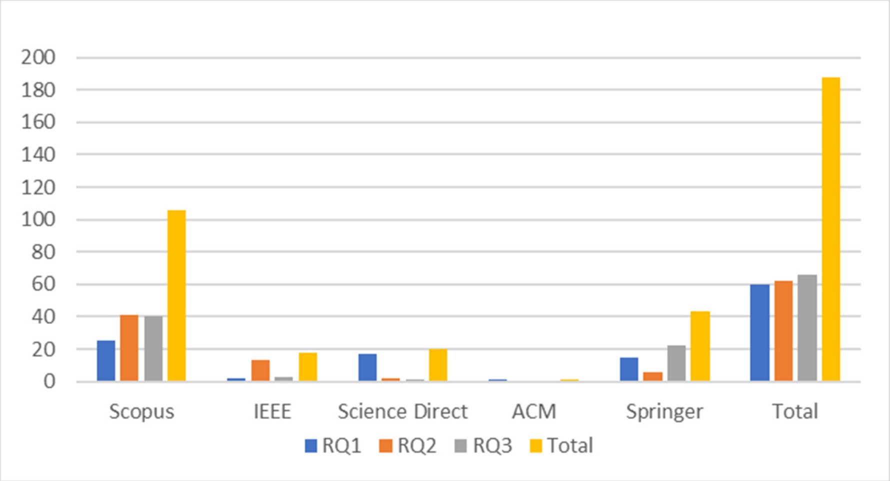

Figure 7. Statistics of the Search Process.

3.3. Documenting the Search Strategy

This phase involved the collection of studies outlined by the search strategy. Additionally, the information acquired from the search technique utilized to retrieve records based on the specified search phrase was recorded. This information included the search date, the name of the online library, and the total number of retrieved items. This stage reports all relevant information regarding the searched papers. This documentation supports the search evaluation and enables search tracking [86]. Table 6 illustrates the entire process of recording the search in detail.

Table 6. Total Number of Research Studies.

Research Question	Searched Content	Scopus	IEEE	Science Direct	ACM	Springer
RQ1	All Fields	4892	13	12,992	1148	209,949
	TAK *	128	2	22	1	15
RQ2	All Fields	9800	34	3389	257	209,989
	TAK	187	13	13	-	11
RQ3	All Fields	35,574	169	5395	1432	210,974
	TAK	86	3	4	-	48

* Title, abstract, and keywords.

3.4. Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were used to analyze the included papers (see Table 7). The first stage eliminated duplicate publications. Subsequently, each document was compared to the given keywords and study objectives. Some publications were eliminated as they lacked detailed responses to the queries. Each manuscript was evaluated using inclusion–exclusion criteria based on its title, abstract, and complete reading. The research was chosen from peer-reviewed journals and conference proceedings. If numerous versions of the same document existed, the most recent, comprehensive, and updated copy was selected for inclusion, whereas all other copies were eliminated. Conflict analysis was used to avoid duplicates at every selection level.

Table 7. Inclusion and Exclusion Criteria.

Inclusion Criteria	Exclusion Criteria
Research papers in the computer science field.	Research papers that are out of the field of computer science and duplicate papers with fewer than three pages.
Research papers published in journals or conferences.	Research papers published in book chapters and workshops.
An English-language research article.	Research papers published in languages other than English, such as Chinese, Turkish, and Spanish.
Research article published from 2012–2023.	Research papers published before 2012.
Research papers related to and answering the research questions.	Research papers that are not related and do not answer the research questions.

3.5. Quality Assessment Criteria

In order to evaluate the quality of the selected studies, one of the most important steps is determining their quality. The assessment of the quality of the studies involves the creation of inquiries aimed at assessing the extent to which the scrutinized articles have tackled partiality and the internal and external reliability [80]. Table 8 presents the five questions that make up the quality evaluation (Q1–Q5), with the possible responses categorized into 1 for yes, 0.5 for partially, and 0 for no.

Table 8. Assessment for Quality of Papers.

ID	Questions
Q1	Are the study's objectives presented in a comprehensible manner?
Q2	It likely that all related studies were included in the literature review?
Q3	Does the study use primary data to support its arguments?
Q4	Does the study provide an adequate explanation of the research method?
Q5	Does the study specifically concentrate on APTs on mobile devices?

3.6. Performing Snowballing and Data Synthesis

The snowballing phase is a systematic literature search method where references or citations in a document are used to locate more articles. This approach enabled the identification of articles relevant to the research and their inclusion as an information source to aid in the understanding and explanation of the study's subject [87]. The data synthesis process, which is the most critical stage in an SLR, aims to address the research questions, synthesize the retrieved data, and report the findings [88]. The publications were classified into designated groups based on the retrieved data to address the associated research topics. Subsequently, the findings were summarized and shown appropriately. The extensive explanations of the reported findings were included to elicit and emphasize the most critical elements of each research issue. Additionally, key results, such as current study directions, accomplishments regarding the use of attention mechanisms, unresolved issues, and recommendations for future studies, are included.

3.7. Paper Selection Process

The study selection process in this SLR comprised five stages in five digital libraries: ACM, IEEE, ScienceDirect, Scopus, and Springer. As seen in Figure 8, 1351 papers were retrieved. In the subsequent stage, exclusion criteria and the removal of the duplicated papers were implemented. Subsequently, a total of 533 articles that were potentially related to the research were retrieved from the online search. The authors particularly focused on research that satisfied the inclusion criteria.

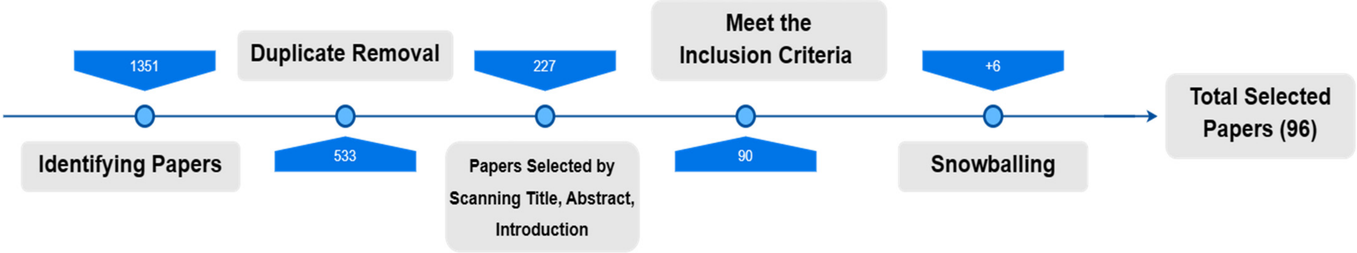
1351
Identifying Papers
Duplicate Removal
533
227
Papers Selected by Scanning Title, Abstract, Introduction
Meet the Inclusion Criteria
90
+6
Snowballing
Total Selected Papers (96)

Figure 8. Paper Selection Process.

A total of 227 studies were analyzed by their titles, abstracts, and overall results. Subsequently, the abstracts and the conclusions of the papers were read, which led to the linked studies before the quality evaluation was undertaken, resulting in a total of 90 studies being selected. The snowballing approach was performed (forward and backwards) by adding six more papers to the selection process. Only 96 articles were chosen and discussed as potential data synthesis sources.

The selection was accomplished by first applying exclusion criteria to remove irrelevant or duplicate papers and, subsequently, applying a filter to the results of the quality assessment stage applied to all the papers.

4. Analysis and Findings of Research Questions

In this section, each research question is assessed to determine whether it was answered in detail to fulfill the research objectives precisely. The analysis for each research question is presented below.

4.1. Research Question 1: What Activity Is Carried out by the User on a Smartphone That Is Highly Vulnerable to Security Attack?

This research question aimed to assess user activities and behaviors the attacker could exploit to compromise smartphones through sensors. The user's activity refers to how they use their device daily (for example, installing applications, clicking a link from an attached file that grants permission to an installed application, and other activities). Such user activities or behaviors, whether intentional or unintentional, may lead to a smartphone being targeted by a cyber attack and the vulnerability of the mobile device being exploited or compromised. The mobile device has certain vulnerabilities, such as small capacity, low-cost sensors, and constantly being switched on.

Several security attacks occur from these vulnerabilities, including AndroRAT, Desert Falcon, and FineSpy. The asset may become an easy target for cyber attacks due to the user's behavior and limited awareness concerning the smartphone's sensors. Furthermore, unawareness can also be due to physical activity, such as leaving the mobile device unattended, leading to theft. Additionally, smartphones are particularly vulnerable to cyber attacks for two reasons: (a) user activity and (b) the development cycle for mobile applications with poor quality.

As Figure 9 and Table 9 illustrate, user activity leads to the targeting of smartphones. Table 9 shows five modalities: sensors, services, physical, software, and applications. Each of them is connected to the related mobile sensors, which indicate the user's activities.

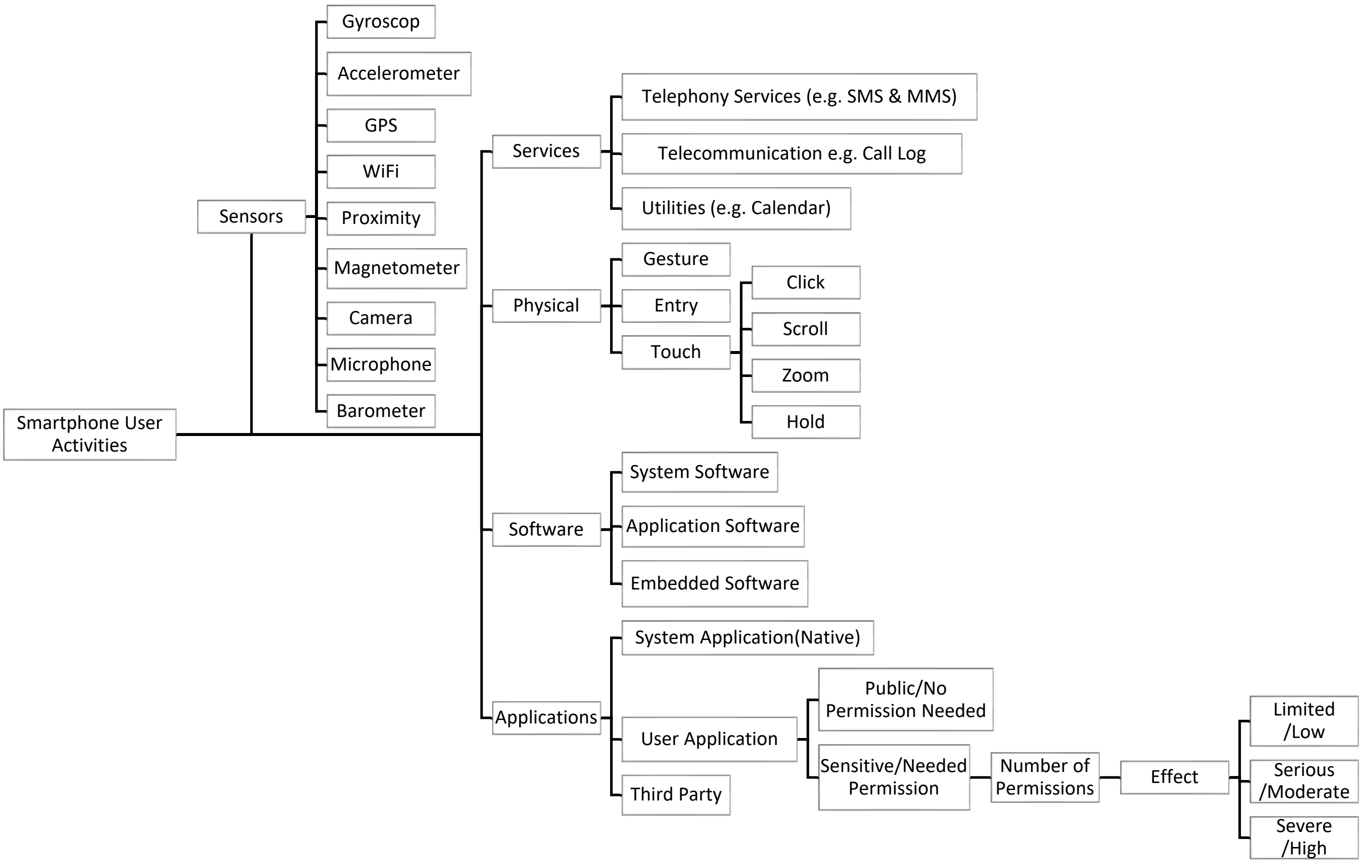

Figure 9. Smartphone User Activities Classifications.

4.1.1. Smartphone User Activities Based on Sensor Modality

In several studies [89,90], the survey aims to illuminate various activities, including storing personal passwords on the phone, ensuring that the mobile device software is updated, obtaining software from third-party websites, and searching for free Wi-Fi. Nevertheless, in research by [91], the user behavior was classified as local device management, network management, and remote service management. Only 36% of smartphone users use a four-digit PIN screen lock, with the remainder using anti-virus software, a PIN or an unlock pattern, data cleansing software, and encryption. Contrastingly, 34% of users do not utilize any such measures.

The network management category specifies how stringent or flexible the user's options are for connecting to unknown communication nodes. Furthermore, both studies by [92,93] focused on behavior targeting the GPS sensor of smartphones relating to the user activity (continuously enabling GPS, Bluetooth, or enabling remote tracking of the device) [93], making a wide landscape for vulnerability.

Table 9. Activities of the Smartphone User.

Modality	Sensors and Method	Activities
Sensors	Positioning (GPS, Wi-Fi, and Bluetooth)	How restrictive or permissive the user's selection of unknown communication nodes is [90]. Constantly enabling GPS, remote device tracking, and Bluetooth [92]. Connecting to insecure Wi-Fi hotspots [87,89,92]. Gaining the user's location through GPS or the position of the closest cell tower [91].

Table 9. *Cont.*

Modality	Sensors and Method	Activities
Services	Telephony Services, Telecommunications	Tapping on a malicious link sent through email, SMS, or an "in-app" advertisement in another app such as a game [12,92,94,95]. Adoption of BYOD policies [96]. Using mobile advertising to communicate with users and collect data from mobile devices [97]. The user uses voice access technologies in mobile devices and voice assistants [98]. Modern vehicles relate to the world around them through Wi-Fi connections or 3G/4G networks [85]. Considering mobile devices as a trusted companion [99].
Physical	Touch, Gesture, Entry	The user's touch actions (tap, scroll, hold, and zoom) and PINs permit a remote website to discover client-side user activity [100]. The user visits a website controlled by an attacker [95]. The utilization of smartwatch and wearable accessories [101]. People regularly carry significant data assets on mobile devices [96]. Downloading suspicious email attachments [92,94]. Uploading location-based data to social media [92,94].
Software	System Software, Application Software	Browsing the latest downloads and interests using device location analysis [75]. Poor coding and validation of input fields [102,103]. Updating software on a mobile device [87,89]. Jailbreaking and rooting mobile devices [87,89]. Utilizing mobile applications known as wallets [104].
Applications	User Application, Third-party Application	Storing personal passwords, social security information, private pictures, and bank account information on a mobile device [87,89,96,105]. Checking permissions that the application requires [87,89]. Downloading apps from untrusted third-party websites [12,87,89,92]. Installing any malware attached to an email [12]. Sharing of PIN, password, or pattern information [92]. Downloading and utilizing third-party app stores, dealing with illegally modified free copies of premium programs [106].

4.1.2. Smartphone User Activities Based on Service Modality

Research has been conducted on smartphone users where such devices were found to store personal contacts and images [107]. Additionally, instructors might use their computers to store academic materials, while numerous businesses have implemented the BYOD approach, permitting employees to link their own devices to the business network [94,108]. The BYOD approach plays a fundamental role in user behavior.

The trend towards bringing personal devices to work has gained traction in organizations, particularly in rapidly growing nations such as Brazil, Russia, and India [109]. Nevertheless, this development has negative aspects in terms of maintaining the integrity and secrecy of sensitive data due to the mobility of devices and the ubiquitous network enabling data to be viewed from anywhere [110].

Modern vehicles are connected to the outside world through Wi-Fi or a third generation/fourth generation (3G/4G) network [95]. It delivers endless benefits to drivers in terms of services and smart functionality. Nonetheless, it poses significant threats to security and privacy, potentially jeopardizing passengers' safety. When the user visits an attacker-controlled website [98], the JavaScript code embedded in the website page starts listening to the gesture and rotation sensors without the user's consent.

Research by [111] showed how users interact with mobile devices and voice assistant systems through voice access technologies. Several studies found that malicious links could be transmitted through email or an "in-app" advertisement within another application, such as a popular game [12,93,97]. Moreover, mobile advertising systems display adverts for local restaurants to consumers using GPS, enabling users to schedule bookings through smartphones. Mobile devices also store diverse data, including geographic locations and contact information, while offering robust functionality such as SMS, phone calls, and 3G or 4G connections [99]. Such information can be abused with sinister motivations.

4.1.3. Smartphone User Activities Based on Physical Modality

Some studies discovered that motion and orientation sensors (gyroscope, accelerometer) might be breached due to a user's behavior [96,98]. Nevertheless, the user uses mobile web browsers, carries out touch actions (tapping, scrolling, holding, and zooming), and uses PINs. Such actions enable a remote website to learn about the user's client-side activities [96].

Other activities potentially leading to mobile phone exploitation include the use of smartwatches and wearable accessories, which expose mobile devices to vulnerabilities [101,112]. Furthermore, people frequently hold mobile phone devices with essential data assets [107]. Apparently, users are inclined to download attachments from unknown sources, share their location through social networking sites, and browse the web while monitoring their devices' most recent downloads and interests [92,93,109].

4.1.4. Smartphone User Activities Based on Software Modality

According to [102], ineffective coding and the selection of ineffective programming software solutions significantly contribute to the unavailability of web application services as attackers exploit the vulnerability of input fields. This condition is accomplished by either putting the SQL query command into the input or appending the query with the desired uniform resource locator (URL). These SQL queries are converted to SQL code that an attacker inserts [102,103].

This vulnerability injection is the primary vector through which an attacker can compromise a web application's security. In addition, rooting and jailbreaking mobile devices are the most dangerous activities leading to smartphone intrusion [89,90]. Moreover, research [104] has indicated that threats emerge due to insufficient validation of user input information, software designed without adhering to stringent safety requirements, and vulnerability of reusable software libraries, among other issues. Cyber attacks do not solely target mobile phones but also the Android system in modern vehicles, referred to as the Android in-vehicle infotainment (IVI) system.

4.1.5. Smartphone User Activities Based on Application Modality

According to [100], users' password-entry activity may be observed by others, captured on small recording devices or public surveillance cameras when they use their mobiles in public. An adversary can immediately access sensitive data if a mobile is stolen or lost, as most user authentication mechanisms do not support post-login authentication. As system usability is crucial [107], user authentication mechanisms are continually constrained by usability and security trade-offs.

In a study by [106], smartphone wallet software frequently facilitated consumer contact with cryptocurrency. Static code analysis and network data analysis were adopted to investigate and reveal that a lower rate of security vulnerabilities characterizes traditional banking applications compared with cryptocurrency applications. Furthermore, Google Play Store and other third-party app shops tackle illegally modified free versions of costly products. The dearth of sufficient security measures permits the rapid proliferation of mobile malware within these markets [113]. Moreover, one of the most pervasive and severe errors on these devices is the digitalized copies of traditional agendas and contact books. They are also the primary and ultimate interfaces to what is popularly referred to as the "mobile cloud" [103].

Relevant to the first research question, smartphone users' activities have been categorized into five groups: sensors; services; physical; software; and applications. Each group is associated with the activities or behaviors connected to the sensors based on the permission granted. Notably, user behaviors contribute to cyber attacks due to unawareness, lack of knowledge, and unskilled employees inside a business, resulting in targeting smartphone assets such as contacts, bank information, and images. Providing permissions requested by applications exposes the mobile user to privacy threats [114].

Email, services, and sensors are the mediums for spear phishing on mobile devices.

The sensors serve as a means for data exchange, shared services provision, and message transmission between various electronic devices.

Nevertheless, attackers can take advantage of this vulnerability to attack by either sharing malicious links or sending malware to a targeted victim in the form of an .apk file. Victims are more likely to click a URL than malware since malware needs to request access to specific permissions, such as the Internet, to obtain access to the data [53]. Consequently, smart devices face numerous issues due to threats that can be easily implemented, gain access to the sensors, and be exploited due to a lack of awareness.

Researchers have proposed numerous solutions to strengthen smartphone security against sensor-based threats. These solutions range from imposing strict permissions for sensors to analyze information flow between devices. On the other hand, these suggested solutions rely on either the decisions made by users or the accessibility of the applications' source code [115].

4.2. *Research Question 2: What Are the Detection Mechanisms of APT Attacks on Mobile Phones?*

An APT is a sophisticated attack involving infecting a system and remaining there for a lengthy period to hack personal data. When APT assaults are launched against a dynamic and complex infrastructure, typical detection approaches can be extremely challenging to adopt [116]. Defending against an APT attack using only a single tool is impossible. Adopting the "defense-in-depth" approach establishes a system that can identify and stop an APT attack at every stage, irrespective of location or network layer.

The correlation of events generated by these various protection methods is critical for defending an organization or entity against APT assaults. This research question pinpoints the mechanism to identify APT attacks on smartphones, as presented in Table 10. Notably, different cyber attack types target specific platforms, such as personal computers, the IoT, cloud computing [117], and smartphones. Various detection mechanisms to identify advanced persistent threat (APT) attacks have been explored. However, these studies have only partially solved this problem, as they often fail to detect all attack stages. In addition, some approaches have proven ineffective at efficiently detecting the attack in its early stages, resulting in substantial damage being inflicted before detection occurs. This is primarily attributed to APT attacks' stealthy, sophisticated, and evolving nature. Moreover, the attack's behavior is intentionally designed to resemble normal activities, employing a "low and slow" approach, which further complicates the detection process [118].

As illustrated in Figure 10, APT defensive strategies have been classified into three broad categories: monitoring, detection, and mitigation. Each category or class can be classified further.

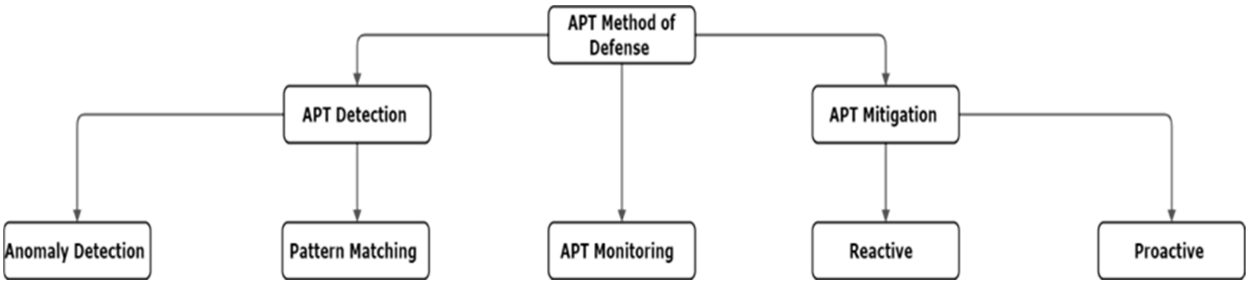

Figure 10. APT Defense Method Classifications [16].

4.2.1. Personal Computer APT Detection Mechanisms

In research by [119], a cyber kill chain approach was adopted to detect an APT on a personal computer. Utilizing an industry-recognized cyber kill chain technique for dataset reconstruction enabled improved resolution of the attack phases and alert types, which are crucial for APT attack analysis. Notifications were carefully organized, with one warning potentially correlating to numerous attack phases determined by the APT lifecycle within the cyber kill chain framework. While identifying APT attacks, the authors [120] devised a novel technique entitled APT-Dt-KC. Bayesian algorithm classification prioritization and selection were implemented to select training data and significantly increase the runtime efficiency.

According to research by [121], deception is a potential strategy for detecting assaults. This approach can identify attacks irrespective of the attacker's skill and ability levels. Additionally, it provides a comprehensive APT detection methodology, implements it, and tests it against two scenarios. Furthermore, in research by [122], the fractal dimension-based machine learning classification strategy was implemented for APT detection. This approach proposed utilizing the transmission control protocol/Internet protocol (TCP/IP) feature vector to mitigate APT effects. The authors posited that their technique outperformed more established machine learning methods, for instance, the K-nearest neighbor (KNN) algorithm. Additionally, the authors of [23] proposed a distinctive machine learning approach named MLAPT, which is capable of systematically detecting and forecasting APT assaults with high accuracy and speed.

Some studies presented the definition of network genes, an innovative network application technique that integrates the semantically rich activity characteristics model [123]. It is feasible to assess a network entity action's identity significance and source similarity to identify network applications by matching network activities to network genes. Similarly, an effective anomaly-based detection strategy for robots and APTs was investigated using a data mining technique with applicable classification techniques [124].

Furthermore, spatiotemporal association analysis was identified as a method for detecting an APT attack within an industrial network, enabling the successful identification of the APT attack's stealing behavior [19]. Several researchers proposed detection mechanisms using network traffic flow with a combination of one of the machine learning algorithms, such as support vector machine (SVM), with deep learning undertaken to detect, monitor, and analyze the APT attack in the system [117,125–127].

A strategy for identifying APT attacks based on monitoring access to unfamiliar domains was previously proposed by [116]. As a recently developed IT technology, big data technology provides several technological advantages for Internet-enabled applications while potentially providing excellent framework support for APT detection [128]. In studies by [129,130], situation awareness models have been adopted to detect APTs.

An APT alerts and logs correlation technique (APTALCM) has been recommended to accomplish cyber scenario understanding. Initially, a cyber scenario ontology was developed to model ideas and attributes to formalize APT attack operations and detect APT attack goals. It was presented to measure the similarity of cyber scenario cases based on the SimRank approach [131]. Nevertheless, a study by [132] presented APTPMFL, a federated learning-based APT prediction technique for fifth generation (5G)-enabled IoT. Training a model using various APT attack patterns was undertaken using a distributed learning technique. The final result was used to anticipate the likelihood of future APT attacks in 5G-enabled IoT scenarios.

Table 10. APT Detection Mechanisms.

Platform	Detection Mechanism	Description	Article
PC	Cyber Kill Chain	A technique for reconstructing datasets to enhance the resolution of attack phases and warning types.	[119]
	APT-Dt-KC/Cyber Kill Chain	Analyzes, identifies, and prevents cyber attacks using the cyber kill chain concept and its fuzzy features against an APT assault.	[120]
	Fractal Dimension	A fractal-based APT detection method leveraging the TCP/IP feature vector to mitigate the APT's impact.	[122]
	Machine-Learning Correlation Analysis	A novel machine learning-based system named MLAPT.	[23]
	Machine-Learning with XGB Classifier	Machine learning techniques, specifically the XGB classifier, in conjunction with the ANOVA feature selection method.	[133]

Table 10. *Cont.*

Platform	Detection Mechanism	Description	Article
PC	Graph2vec Algorithm and Deep Learning	Profile analysis and an APT malware detection model utilizing the graph2vec algorithm and deep learning.	[134]
	Evasive Maneuver Re-Engineering Framework (EMRF)	Demonstrates how evasion techniques can be used to bypass modern security solutions.	[135]
	POIROT	Utilizes causal correlation-aided semantic analysis to detect multistage threats based on alerts.	[118]
	A Network Gene-Based Framework	A novel concept illustrating the network application's semantically rich behavior characteristics model.	[123]
	Flow Network Analysis Techniques	A novel deep learning-based approach for detecting APT assaults through network traffic.	[125]
	Unknown Domains	A technique for identifying APT assaults that relies on monitoring access to unknown domains.	[131]
	Big Data Processing	The big data processing technique provides several technological advantages in the realm of Internet-enabled applications.	[128]
	Network Traffic Analysis	An approach for analyzing unusual network traffic using a machine learning approach.	[127]
	APT Alerts and Logs Correlation	APTALCM, an APT alerts and logs correlation method, is adopted to establish an understanding of the current cyber scenario.	[129,130]
	APT Prediction Method (APTPMFL)	Federated learning-based approach for predicting APTs (APTPMFL).	[132]
	Data Mining Approach	Investigates the properties of packets and flows, among other aspects of network traffic.	[124]
	Algorithm Based on Spatiotemporal Association	Usin a spatiotemporal association analysis, how the APT assault is stealing information is determined.	[19]
	Captured Network Traffic Data	Investigates the adoption of an algorithm built from flow-based monitoring as a substitute for the traditional security strategy.	[117]
	CONAN	FSA-like state transition technique detects APT attacks efficiently and accurately.	[136]
	MITRE ATT&CK through Open Source EDR	Attack detection and coverage analysis were feasible during all APT attack stages.	[137]
	Semi-supervised Learning and Complex Networks Characteristics	Identifies a susceptible host from a network of hosts suspected of participating in APT activities.	[138]
	Clustering Algorithms	Uses suitable clustering approaches such as APRIORI, K-means, and Hunt's algorithm to identify sophisticated APTs.	[139]
	Multistage Autoencoders	Investigates several anomaly detection methods.	[140]
Mobile	Network Traffic Monitoring	A method for monitoring network traffic that is used to detect Android malware.	[126]
	Typosquat	Investigation of how APT attacks occurred on smartphones through URL hijacking.	[53]
	Deception Approach	A potential strategy for detecting attacks irrespective of the attacker's capabilities.	[121]
	Ensemble Learning	Uses a decision tree and neural network to categorize the URL.	[141]
	Large-Scale DNS Logs	Analyzes DNS logs to detect APT mobile assaults.	[142]
	Mobile DNS Logging	Uses mobile DNS logging to identify APT attacks.	[143]
	Control Flow Analysis	Describes how to perform a kernel modification APT attack.	[144]
	5G Slicing	A new technique that will be adopted in 5G networks.	[145]
	Leave One Feature Out (LOFO)	Selects key Android app characteristics for malware detection.	[146]
	TriggerScope	Identifies logic bombs by defining the checks that protect a particular behavior.	[147]
	DDefender	An app investigating Android apps statically and dynamically.	[148]
	Using Mobile Phones as the Detector	A mobile device implementation, making it adaptable to other services besides notifications.	[149]

Table 10. *Cont.*

Platform	Detection Mechanism	Description	Article
	MITRE Framework	Utilizing the TTPs framework of MITRE for mobile for mitigate the occurrence of false positives.	[150]
IoT	Kalman Backpropagation	Kalman backpropagation is used to design a dynamic predictive model.	[151]
	Machine Learning Algorithm	The suggested method is dependent on machine learning algorithms.	[152]
	Local Outlier Factor (LOF)	Recognizes suspicious behavior that differs from what is expected.	[153]
	Intelligent APT	Presents an intelligent APT detection and classification system for securing I-IoT	[154]
	Honeypot	The honeypot acts against APT attacks in SDN through the DBHM model.	[155]

Moreover, Ref. [136] presented CONAN, which delivers rapid and effective APT attack detection using an FSA-like state transition technique. A revolutionary framework for state-based detection was introduced, through which each process and file is represented as a well-designed data structure for real-time, long-term detection. For the first time, a study of open-source EDR enabled attack detection and coverage analysis for all APT attack phases, as defined by MITRE ATT&CK [137].

Several stages had a poor detection rate as a consequence of insufficient query parameters to identify detailed stage-specific assaults. The Teach model was implemented to undertake an in-depth performance evaluation, investigating assaults with high significance and low detection levels. Lastly, a semi-supervised learning strategy and complex network properties were introduced to demonstrate the evolution of the APT-AN [130].

A study [133] introduced a method for identifying APT attacks through the utilization of a recently constructed dataset specifically designed for these attacks. The dataset was utilized in a proposed machine learning model to identify APT attacks based on various attack categories. The study gathered five distinct categories of data, specifically normal, reconnaissance, initial compromise, lateral movement, and data exfiltration. Each type of data signifies a particular phase that the perpetrator could have potentially reached. The proposed model for detecting APT attacks utilizes machine learning techniques, specifically the extreme gradient boosting (XGB) classifier, in conjunction with the ANOVA feature selection method.

Meanwhile, another study [134] aimed to develop a model for detecting APT malware on workstations through early detection and warning. The proposed approach involves utilizing the graph2vec graph analysis algorithm and deep learning models to conduct profile analysis and build the APT malware detection model. This study addressed three problems through its research findings. The process profile of APT malware has been graphically represented to comprehensively illustrate its behavior. Moreover, the suggestion to employ the graph2vec model has yielded noteworthy efficacy. The process profile has been standardized and represented in a graph format, which has been further embedded to display comprehensive features. This aids in the efficient detection of APT malware.

Additionally, the researchers of [135] conducted a thorough literature review and analyzed publicly available APT samples using multiple analysis techniques, including static, dynamic, and reverse engineering. The study has provided a detailed overview of various techniques used by APT malware to evade detection, such as stealth mechanisms, anti-analysis measures, and covert communication methods. The evasive maneuver re-engineering framework (EMRF) is a newly developed framework by the authors. It comprises several modules, including process injector, DLL hijacker, fileless mechanism augmenters, code obfuscators, anti-debug augmenters, anti-virtualization augmenters, anti-sandbox augmenters, and custom evaders. The framework aims to demonstrate how evasion techniques can be used to bypass modern security solutions and prove their effectiveness.

Finally, the study of [118] has successfully devised a system that consolidates and leverages alerts from pre-existing systems for the purpose of identifying APTs. The proposed system, POIROT, utilizes causal correlation-aided semantic analysis to detect multistage threats over an extended period of time based on alerts from pre-existing systems. The study utilized causality analysis to autonomously identify the logical connections among the alerts, resulting in the restructuring of the initial alerts into alert chains without prior knowledge of APT processes. This approach significantly decreased the number of irrelevant alerts present in the extensive logs.

4.2.2. Smartphone APT Detection Mechanisms

Numerous studies have analyzed smartphones' detection mechanisms, particularly for Android operating system devices and cyber attacks that target the IoT, such as MIMA [147]. Studies by [53,141] investigated how an APT assault through spear phishing may occur on mobiles through URL hijacking by seeking to explain how they can be identified. The machine learning approach has achieved over 90% accuracy. This finding confirms that it has the ability to help mitigate APT attacks through spear phishing on smartphones [53]. An APT guard attempt was proposed to categorize the URL using a decision tree and neural network [141].

In works by [142,143], mobile domain name system (DNS) logging was used as an APT detection technique. Specifically, a method for APT attack detection on mobiles, based on analyzing DNS logs using a machine learning technique, was proposed [142]. According to the researchers, the DNS of the APT software on cell phones and laptops differs markedly. On the other hand, Weina Niu et al. [143] developed a technique for detecting APT attacks based on mobile DNS logging, which draws on four distinct datasets, including request of DNS, reply, and domain time-based features.

A study [144] proposed a method that detects APTs by analyzing control flow of the binary code of the kernel. The control flow analysis compares the genuine kernel's control flow graph with the device kernel's control flow graph. It detects APTs using the fingerprints generated during the detection procedure.

TriggerScope, a first step towards the automated detection of logic bombs, was suggested by [147]. It employs a novel static analysis approach for automatically detecting triggers in Android applications. DDefender, a user-friendly program for identifying dangerous Android applications on devices, is presented by the authors of [148]. DDefender employs a comprehensive solution that utilizes static and dynamic analysis approaches to extract information from the user's device.

Subsequently, a deep learning algorithm was utilized to detect harmful programs. Finally, in research by [149], an enhancement of an escalation data analysis (EDA) was proposed. It is a technique for automating the detection of APT assaults that breach a node within an organization to steal data.

Finally, Ref. [150] presents an automated system that specifically targets cyber attribution. The study was conducted utilizing the TTP framework of MITRE for mobile. Through the comparative analysis of the indicator of compromise (IoC), it was able to effectively mitigate the occurrence of false positives in the experimental study. Moreover, the automated method for detecting cyber attribution has been utilized to scrutinize 12 threat actors and 120 malwares. The implementation of this technology will facilitate the automated classification of tactics, techniques, and procedures (TTPs) for a multitude of mobile threats. Furthermore, through the provision of TTP and IoC pairs to the analyst, it becomes feasible to classify and identify potential mobile attackers.

4.2.3. IoT Device APT Detection Mechanisms

In a study by [145], 5G network slicing is explained, and a technique is developed for isolating user device testing on a dedicated test network slice. This concept permits the detection and analysis of the most sophisticated malware on a device. Furthermore, a detection solution for Android malware based on the leave one feature out (LOFO) principle was introduced [146]. The suggested technique is designed to select essential Android application properties for effective Android malware detection by training several tree-based classifiers at the lower level.

In some studies, detection techniques were applied to smartphones as part of the IoT network [151,152]. They provided a distributed denial-of-service (DDoS) intrusion detection model that is deployable in dynamic IoT settings. Thus, it provides an intelligent intrusion detection technique against the second most serious threat to data transit and transfer on IoT networks [151]. A strategy dependent on machine learning algorithms for optimizing the time required to identify a MITM in a network was also presented [152]. A technique for detecting and classifying APTs in I-IoT was provided by [154].

Numerous machine learning techniques were adopted to identify and categorize dangerous IoT devices vulnerable to APT assaults. In order to develop such a system, the dataset KDDCup99 was utilized. The comparison of machine learning approaches revealed that the AdaBoost classifier surpasses the others with 99.9% accuracy and a 0.012 s execution time for identifying APT assaults, which is acceptable for usage in the I-IoT area. Moreover, a local outlier factor (LOF) and an autoencoder were devised for detecting suspicious behavior deviating from usual behavior [153]. Additionally, DDefender identifies and displays associated dangers by analyzing suspicious events and matching them against the conditions defined in the attack profile.

Lastly, in [121], bounded rationality was presented in the SDN-based honeypot dynamic defense APT. The simultaneous dynamic attack and the defense process using the prospect theory were modeled. The dynamic interaction between the attacker and the defender has been formulated using a DBHM, and the bounded rationality has been expressed through a Prelec function and a weighting function.

Based on the analysis of studies regarding the second research question, it is observed that various techniques are used to detect APT attacks targeting computers and smartphones. While existing techniques for detecting APT attacks have attempted to provide solutions, they have not been entirely successful due to a lack of focus on human behavioral factors and the complex nature of APT attack trails or TTPs.

The APT defense solutions have centered around recognizing, preventing, spotting, and counteracting APT attacks. Machine and deep learning are the most popular methods to detect APT attacks. Threat scenarios from APT malware, such as ZooPark, are constantly evolving, posing difficulties for existing detection methods to keep up. Due to the dynamic nature of the threats faced, it has been unfeasible to develop a complete picture of the TTPs of APTs [32].

Notably, most APT detection methods have concentrated on the communication channel between the attacker and the C&C server. The component of APT malware in question plays a crucial role in receiving persistent instructions and the exfiltration of stolen data. Host–server interactions typically occur at low and slow rates and are frequently camouflaged as regular packets of network traffic. The hypertext transfer protocol (HTTP) is used for most communication and generally behaves similarly to any other form of network traffic. Over 90% of APT intrusions use the HTTP for communication. The main benefits an attacker can reap from using the HTTP for network-wide communication are convenience and ease of access. First, the communication protocol is used by all organizations worldwide. Second, it generates massive web traffic, which hides malicious activity and bypasses the organization's firewall [39].

4.3. Research Question 3: What Challenges and Problems Might Appear in Adopting AI Techniques for Detecting APTs in Mobile Sensors?

Two groups of platforms emerged from the studies that answered the third research question, with personal computers and smartphones being the most prevalent targets of AI techniques.

4.3.1. AI Techniques/Algorithms Used to Detect APTs in Personal Computers

The relevant research regarding this question has been observed to include different types of cyber attacks targeting specific platforms, such as personal computers and smartphones. On the one hand, as observed in Table 11, the AI techniques used against personal computers were machine learning [23,119,122,156,157], deep neural networks [158], game theory [159–168], fuzzy neural networks [169,170], and anomaly detection [123]. In research by [112], several machine learning classifiers were adopted, including naïve Bayes, Bayes net, K-nearest-neighbor (KNN), random forest, and SVM.

Additionally, Weka performance measures were employed to display the numerical findings. The primary obstacle was the minimal number of features of the dataset. This situation was addressed by extracting features and selection techniques. In contrast, Ref. [163] offered an anti-phishing system with the ability to identify phishing URLs in real time without third-party information and in a very short response time. This method was designed to detect phishing assaults with high accuracy based on a limited number of characteristics.

The evaluation used four distinct algorithms: random forest, K-nearest-neighbors, logistic regression, and SVM. Ghafir et al. [23] recommended a MAPT model based on machine learning for detecting APTs. It is divided into three parts: detecting threats, predicting attacks, and alert correlation. This study presents MLAPT, a unique machine learning-based method with the ability to predict APT attacks. Furthermore, a study constructed a fractal-based machine learning algorithm to enhance phishing detection approaches [122] by utilizing machine learning techniques [157].

It is recommended that an AI-enabled APT detection system based on blockchain is used to defend against the forging of industrial IoT data [171]. Incorporating reusable machine learning methods at the IoT edge protects information before its transmission in cyber space. One study applied a deep embedded neural network expert system (DeNNeS), enabling extraction of improved regulations from an educated deep neural network design to replace an expert system's knowledge base [158].

Moreover, the present study of [172] aimed to enhance the efficacy of APT malware detection on endpoints. To achieve this objective, the researchers have developed the GECA combined model utilizing the intelligent cognitive computation approach (a combination of GE and CNN-Attention). The model has been successfully constructed. The optimization of two problems through the implementation of intelligent cognitive computation techniques has resulted in an enhanced capacity for malware detection. Initially, the technique of extracts behaviors of APT malware through process analysis. Secondly, the techniques employed for detecting APT malware are based on behavior analysis. The proposal has effectively introduced a GE network that is grounded on the graph convolutional network (GCN) for the purpose of synthesizing and extracting malware behaviors that are process based.

A computational system based on intelligent hybrid models was proposed and constructed by [158]. It enabled the development of expert systems with the capability to attack various sorts of cybernetic data by utilizing fuzzy rules. Nevertheless, a study conducted by [170] attempted to identify and predict unknown "zero-day" phishing emails through the introduction of a novel framework known as the phishing evolving neural fuzzy framework (PENFF). It focused primarily on using evolving fuzzy neural networks (EFuNNs). A gene-based technique comparable to traffic data analysis was applied to identify the APT. It recognizes certain similarities to APT assaults by utilizing the pattern of previously occurring attacks. This approach was paired with anomaly detection [123].

In [156], a machine learning and malware-based classification scheme for APT groups was suggested. This technique relies on behavior data annotated with APT organization tags gathered from the dynamic analysis of APT malware on IoT devices to generate relatively robust feature vectors through feature representation and feature dimensionality reduction.

Meanwhile, Ref. [173] presents a novel approach for identifying APT malware on workstations. This approach involves analyzing the behavioral profile of malware through the use of a deep learning graph network. The study successfully proposed three initial objectives. The paper proposes anomalous behaviors as a basis for process classification and reports that supervised machine learning algorithms and deep learning models have yielded favorable and consistent outcomes. The novel concept of scrutinizing and extracting malware conduct through processes in event IDs has yet to be posited by any scholarly inquiry. The development of an effective behavior profile facilitates the monitoring system's ability to extrapolate and amalgamate not only the procedures engendered by a given executable file, but also the interconnections among said procedures and their corresponding levels of risk.

Moreover, Ref. [174] presents an algorithm for generating adversarial examples in the APT domain. The algorithm was successfully utilized to execute a gray-box attack on an APT detection model. The findings demonstrate that the emergence of adversarial examples can be attributed to the elevated linearization of the targeted model. Furthermore, the transitive nature of the adversarial example has been established, which has enabled the successful implementation of a black-box attack on the APT detection model. The production of APT adversarial examples that have achieved success suggests that a potential avenue for future research in the realm of APT attack detection will involve developing effective defense mechanisms against potential adversarial attacks.

Additionally, Ref. [175] presented a novel methodology that utilizes a fusion of deep learning networks and attention networks. The study outlines a proposed methodology for detecting APT attacks, which is delineated as follows: initially, all network traffic data undergo preprocessing and are subsequently subjected to analysis by the CNN-LSTM deep learning network. This network is a fusion of a convolutional neural network (CNN) and long short-term memory (LSTM). Subsequently, rather than being employed directly for categorization purposes, the data are scrutinized and assessed by the ATTENTION network. Ultimately, the ATTENTION network's output data are utilized for the purpose of APT attack identification.

A study [176] has put forth a novel approach for classifying malware that is based on deep learning. This approach integrates time sequence features and association rule features to achieve its objective. The study employed the RESNET_LSTM and PARALLEL_LSTM neural network architectures, which have been enhanced for improved performance, to extract temporal features from diverse protocol traffic. Moreover, it employed association analysis for the purpose of producing rule features that are quantitative in nature. Ultimately, the time sequence feature vector and the quantization rule vector were integrated as inputs into deep learning models for the purpose of identifying malicious network traffic.

Several studies investigating the adoption of game theory as an AI technique to detect APT on personal computers have been reviewed. Nevertheless, due to the unpredictability of attack durations and the wide range of possible detection outcomes, there are challenges to using this approach effectively. Researchers [159] used cumulative prospect theory to analyze APT detection and the effect of end-users' subjectivity in detecting APTs during unknown assault durations.

In another study, a dynamic gaming framework was devised to present the long-term interplay of a stealthy intruder and a proactive defender [160]. A multistage game of incomplete data, where each participant possesses secret knowledge unknown to the other players, captures the stealthy and deceitful behaviors. The major problem of this technique is determining the value and practicability of the activities of defenders and users during each stage.

Table 11. AI Technique Algorithms Used in Detecting APTs on Personal Computers.

Techniques/Algorithms	Article
Machine Learning	[23,119,122,156,157,171]
Deep Learning	[158,172,176–178]
Game Theory	[159,161–168,178–184]
Fuzzy Neural Networks (FNNs)	[169]
Adoptive Evolving Fuzzy Neural Networks (EFuNNs)	[170]
Support Vector Machine (SVM)	[119,156]
K-Nearest-Neighbors (KNN)	[119,156]
Logistic Regression	[156]
Naïve Bayes	[119]
Random Forest	[119,156]
Bayes Net	[119]
Fractal-Based Machine Learning Algorithm	[122]
Learning-Based Aggregation Analysis Mechanism	[157]
Embedded Deep Neural Network	[158]
Anomaly Behavior Detection	[123]

A study by [161] included a game model that was developed to deal with the issue in accordance with the APT attack route. Before presenting the optimal defensive strategy, the game equilibrium was calculated and the attacker's best revenue path was generated. Dynamic information flow tracking (DIFT) has also been suggested as an APT detection method. This study created a dynamic information flow monitoring game for resource-efficient detection of APTs, using multistage dynamic games [162,177]. In [163], the evolutionary game theory was adopted to illustrate the ongoing long-term activities of APTs on cloud storage.

Furthermore, a hyper-game involving an attacker and a defender has been developed. The actors may perceive the same game differently and select their optimal strategy according to their individual perspectives [164]. A basic framework that splits a generic APT into three primary temporal periods was also presented in a study [165]. The DIFT has been presented as a viable approach for detecting and preventing various cyber attacks in computer systems [166].

The authors of [146] proposed an explainable APT edge protection method. Their recommended approach provides instructions and explanations for constructing the edge defender's protection strategy and resource allocation system to identify APTs. It amalgamates edge gaming and AI techniques based on APT attack intelligence to present a solution and an explicable foundation for an edge defensive system and resource allocation.

In the publications by [167,168], a fog computing platform was used to develop a novel game technique for cyber risk management. The cyber insurance concept was adopted to transfer cyber security threats from the fog computing platform to a third party. Accordingly, three primary entities comprising the system model were under consideration: the fog computing provider, the attacker, and the cyber insurer.

In addition to that, Ref. [178] has examined a particular scenario wherein APT attacks are utilized to launch attacks against industrial Internet of Things (I-IoT) devices. A node-level state evolution model has been developed to assess the likelihood of compromise by an APT across all devices within an industrial Internet of Things (I-IoT) system, taking into account the APT's lateral movement. The study proposes a Stackelberg game model for the APT attacker and defender, which effectively captures the dynamics of the gaming process. A continuous-time propagation model has been established to depict the lateral movement in I-IoT devices. Subsequently, a Stackelberg game model is formulated to depict the sequential interaction between the APT attacker and defender.

A study [180] presents TI&TO, a two-player game that simulates a realistic scenario wherein an attacker and a defender compete for control over resources within a contemporary industrial architecture. The validation of opinion dynamics through the lens of game theory serves to illustrate its efficacy as an initial countermeasure for mitigating and reducing the impact of the APT on infrastructure in the majority of instances. The proposed methodology presented a theoretical scenario aimed at demonstrating the efficacy of the approach across various attack models. The study leveraged concepts from the field of structural controllability and game theory to support its findings.

Finally, the study presented in [181] examines the dynamics of the interaction between a cyber forensic investigator and a strategic attacker through the lens of game theory. The present study pertains to a Bayesian game of incomplete information that is conducted on a multihost cyber forensics investigation graph, wherein both players traverse a series of actions. The classification of attackers into two distinct types has been established, including those that employ anti-forensic measures and those that do not. This categorization is derived from a probabilistic model that is constructed using historical incident reports. The investigator can formulate an effective investigative approach, known as the investigator's optimal randomized plan (IRP), by factoring in the ambiguity surrounding the attacker's classification and the potential benefits and costs associated with each course of action.

4.3.2. AI Techniques/Algorithms Adopted to Detect APTs in Smartphones

According to the data presented in Table 12, the AI techniques adopted concerning smartphones were machine learning, deep learning, game theory, and deep conventional neural networks. Research by [53] investigated how APTs on mobiles may be undertaken through spear phishing through URL hijacking and how they may be detected. The technique achieved over 90% accuracy.

Table 12. AI Technique Algorithms Adopted for Detecting APTs on Smartphones.

Techniques/Algorithms	Article
Machine Learning	[26,53,142,182–184]
Deep Learning	[148,184,185]
Naïve Bayes	[183]
K-Nearest-Neighbors (KNN)	[183]
Game Theory	[159]
Support Vector Machine (SVM)	[183]
Logistic Regression	[183]
Deep Neural Network	[116]
Gradient Boosting	[183]
Federated Learning (FL)	[186]
Deep Convolutional Neural Networks (CNNs)	[187]
Double Q-learning (DQL)	[188]

However, the study's shortcoming was the limited dataset and the usage of only a single user's browser history. According to [142], the DNS of APT attack software on mobiles and PCs is vastly different. Despite adjusting the canopy and K-means clustering method characteristics, the detection impact failed to fulfill expectations, while there was a limit to the number of extracted features.

The authors of [182] introduced OmniDroid, a comprehensive collection of characteristics collected from 22,000 genuine malware and goodware samples, to support developers and researchers in producing anti-malware solutions by enhancing or creating novel procedures and tools for Android malware detection. Nevertheless, the study was limited to investigating the Android operating system. Furthermore, there is an opportunity for improving the OmniDroid dataset, with the dataset of OmniDroid being restricted in terms of the number of retrieved features and samples.

Several studies investigated the effectiveness of deep learning in identifying AI [148,183–185]. The user-friendly Android application DDefender was presented. It has the capacity to detect malicious apps on devices [148]. Nevertheless, the study's weakness was that it examined 4208 distinct programs, with a 50/50 mix between benign and malicious code. Realistically, this distinction is not adequate. The dataset should be expanded to include additional non-malicious programs, as there are many more.

In [183], the authors recommended BetaLogger, an Android-based application, as a solution to address the issue of the leaking of smartphone users' private information. This study's shortcoming indicates that it must be strengthened with additional advances in deep learning, permitting the model to make predictions down to the sentence level.

As recommended by the authors of [184], DeepAMD is an effective and functional means of detecting and identifying Android malware on both the static and dynamic detection levels. The study's focus on the Android OS and its susceptibility to new types of attacks is a limitation, considering the widespread use of iOS on millions of devices.

The paper by [185] presents a new 5G-orientated cyber security architecture to swiftly and efficiently identify cyber threats in 5G mobile networks. The architecture uses deep learning algorithms to investigate network traffic and extract information from the flows to achieve this condition. In order to effectively comprehend how a cyber system and an APT attacker interact, the researchers employ the cumulative prospect theory (CPT) to examine the two parties' interactions [159].

Furthermore, a defense mechanism against APTs has been suggested by [188], which relies on the double Q-learning (DQL) algorithm of MFC. Prospect theory (PT) is employed to construct a stationary subjective game model that involves APT attackers and lawful users. Furthermore, a dynamic game model utilizing double Q-learning (DQL) is suggested as a countermeasure to APT attacks. Ultimately, the study conducts a comparative analysis between the proposed approach and established methodologies, namely the Q-learning algorithm, Sarsa algorithm, and Greedy algorithm. The findings of the experiment demonstrate that the suggested approach is capable of efficiently mitigating the attack inclination of APT attackers, enhancing the usefulness of authorized users, and safeguarding the security of the fog computing environment.

The authors of [187] proposed a unified architecture for early detection of DDoS attacks organized by a botnet that controls rogue devices by utilizing deep convolutional neural networks (CNNs) and actual network data. As there were constraints in the dataset, this study aggregated three hours of data within approximately 60 days and treated them as previous data from a ten-minute slot. The authors of [186] have devised an architecture called Fed-IIoT to identify Android malware in I-IoT. Fed-Android IIoT's malware detection system, which includes different identically distributed learning models, is mandated.

This research faced a significant barrier regarding the most pervasively adopted and well-known mobile operating system for processing and communication. Installing an Android operating system on IoT-based platforms may improve access to a broad range of apps.

Expanding threat detection for a malicious mobile application is vital to analyze risks and provide decision makers with situational awareness [26]. The study presents a method for analyzing threats based on extracted characteristics derived from Android malware detection through fundamental machine learning techniques, such as risk modeling and factor analysis of information risk (FAIR). Furthermore, the study discusses the relationship between mobile risks and cyber space, threat assessment, and the limitations of mobile malware detection.

Moreover, this article presents frameworks for the threat assessment technique based on situational awareness. The findings of the threat assessment for Android malware applications were discussed in the outcome of the threat assessment section. Finally, a study developing a deep autoencoder neural network aimed to classify APT attack types [116]. This model's advantage is its high classification rate by discovering intricate relationships between database characteristics. Apparently, lowering the quantity of data in the encoder facilitates the classification of massive amounts of data.

Based on the evaluation of research studies related to the third research question, several challenges were identified regarding using AI techniques to identify APTs in smartphone sensors. Machine learning and deep learning were found to be popular AI approaches, particularly on smartphones. Notably, there is a lack of studies using game theory or fuzzy logic as an AI strategy for detecting APT attacks on smartphone sensors.

Detecting and preventing APT attacks can be challenging due to their complex nature and the limited understanding of potential attack paths.

Additionally, utilizing AI approaches for smartphone APT detection involves numerous challenges, including a lack of training data, restricted smartphone resources, mobile platform heterogeneity, adversarial attacks, and privacy concerns. A comprehensive analysis of the technological considerations involved in building effective and efficient AI-based APT detection solutions for smartphones would be required [189–191].

5. Discussion

This SLR comprises a comprehensive literature review of 96 peer-reviewed journal articles covering APT attack defense mechanisms from 2012 to 2023. Journal articles were gathered from various online sources, including Springer Link, ScienceDirect, ACM Digital Library, Scopus, and IEEE Xplore. The authors offered an overview of the challenges and problems of using an AI technique for APT detection in mobile sensors, including a summary of APT features and defense mechanisms. Subsequently, the research gaps and recommendations for future investigations will be presented.

5.1. Research Gaps

This section highlights the significant challenges encountered while analyzing the research studies that addressed the research questions. Several solutions and recommendations were proposed to obtain an efficient and reliable result for APT detection in mobile sensors.

5.1.1. Smartphone Users' Activities and Behaviors

Smartphone users' activities have been categorized into five groups: sensors, services, physical, software, and applications. Each activity is related to several activities or behaviors linked to the sensors based on the permissions granted. Mobile sensors are fundamental in collecting, passing, and processing information within a smartphone application. The sensitive data extracted from the sensors are attractive to hackers. Due to their small capacity, low-cost sensors, and constantly "ON" nature, IoT devices often lack the capability to support complex security mechanisms and algorithms [192].

User behaviors contribute to cyber attacks due to unawareness [12,89,90,93,101,112], limited knowledge [93,98,109], and unskilled employees in a business [89,90,102,104,107], resulting in the targeting of smartphone assets such as contacts, bank information, and images. Consequently, granting permissions requested by applications exposes smartphone users to privacy risks [114]. Furthermore, the user behavior and research findings of [13] have been formalized and validated as providing comprehensive security protection and a mitigation model against APT attacks, such as spear phishing, watering holes, and malware attacks.

Nevertheless, a major limitation of SENSATE is the limited exploration of the human behavioral context concerning intention, device usage, and tasks completed with a smartphone. Resultantly, limited studies have focused on identifying malicious behaviors while a smartphone application retrieves the user's data from sensors [12,193].

5.1.2. Ambiguity in APT Attack Path and Late Detection

Concerning the second research question, it has been observed that numerous APT detection mechanisms have been implemented using various types of platforms, namely personal computers, mobile devices, and the IoT. Although many APT detection solutions and techniques have been designed and implemented, they have failed to provide a comprehensive solution for threat detection [11]. The reasons are the limited significance attached to human behavioral factors leading to APTs, unclear APT attack trail, or TTPs [12]. Additionally, the most recent solutions are generalized based on a group of users rather than single individual protection [194].

The number of APTs has rapidly increased. The primary reason is that APTs are not concentrating on a single loophole within a system that may be detected and removed easily. Instead, they are utilizing a sequence of loopholes in several systems to access high-security areas within a corporate network. In this context, attackers regularly exploit the point where most security attempts go into perimeter protection. The attacker's chances of detection are markedly increased if they have gained access to the system's infrastructure [195].

Additionally, identifying APTs before the attackers reach the final stage, with a low percentage of false alarms and missed detections, remains a concern due to their stealth and deception. According to recent reports, it took US organizations three to six months to discover and control a data breach and prevent further damage in 2018 [160]. Contrastingly, it has been observed that inadequate research has sought to identify APTs as a whole, from reconnaissance through clean-up, despite several studies being conducted to detect an APT assault in one or two phases [16,23].

Such a solution necessitates sophisticated correlation and comprehensive behavior analysis of individuals and systems within and across networks. Finally, several attacks are modeled on APTs, such as the MITRE framework and the cyber kill chain, which comprises the APT lifecycle and the APT detection TTPs [70]. Consequently, security experts are unable to identify an attack as an APT [11].

5.1.3. AI Techniques' Challenges and Dataset Shortage

Based on the analysis of the third research question, several challenges have been identified using AI techniques to identify APTs in smartphone sensors. Nevertheless, AI techniques do not stop zero-day and advanced threats. Various researchers have adopted an array of AI approaches, including machine learning, genetic algorithms, game theory, deep learning, and neural networks. The AI is built on learning from previous examples of malicious software, specifically the malicious software's appearance and behavior.

Novel threats have arrived in the form of zero-day exploits and sophisticated attacks. Currently, APTs are equipped with unique evasion strategies and new methods to activate APIs, besides inventive access approaches to system resources. Although certain APT activities may be sufficiently similar to prior occurrences for AIs to detect them, entirely novel approaches have no such past event. Real defense against advanced and sophisticated threats should not rely on previous infections or attacks [196].

Most research has used AI techniques to enhance malware detection's efficiency or accuracy. The priority of cyber threat intelligence (CTI) has recently turned to preventing accidents. Detecting an attacker's malicious behavior is a different essential technique. Determining whether the discovered result may be expressed as a criterion for responding to a threat is a significant obstacle [26]. Nevertheless, it must have access to appropriate datasets to investigate APTs on smartphone sensors.

The lack of smartphone datasets is apparent from the existing literature. Resultantly, evaluating and detecting security risks and threats are unfeasible without relevant datasets. This situation has proven to be a major challenge in implementing AI for cyber security [197].

5.2. Recommended Solution for Mitigating the Gaps

This section contains recommendations for future research to design a model capable of bridging the research gaps identified in Section 5.1.

5.2.1. Conducting a Situational Awareness Model

Regarding user behavior, it has been suggested to conduct a situation awareness approach that entails a comprehension of attackers, estimating attack impacts, evaluating risks, analyzing circumstances, and formulating effective actions to defend important assets [198]. Gaining situation awareness also necessitates a capacity to comprehend how others respond to their environment [199].

The situation awareness model may be employed at three levels: perception, comprehension, and projection. The TTP design will be investigated, and AI techniques will be adopted. This technique can be used in game theory. Furthermore, repeating defense operations (staff awareness training) can be based on information collected from APT cases elsewhere. It enables prior learning to be interpreted more generally than merely documenting one's own and the direct opponent's previous actions [165].

5.2.2. Utilization of Generic Path

Based on user behavior, TTP fingerprinting of smartphones has been suggested. The fingerprint modules generated will have the characteristics of being adaptive, dynamic, and possessing situational awareness. For identification, access and process situational-based awareness features, and individual, task, and environmental behavior with quantification of sensor application connections, normal profiles and malicious (APT TTP) profiles or fingerprints for the smartphone platform can be built.

The process would involve the organization of APT scenarios and case studies into TTPs, prioritizing each TTP risk, and learning the user's cognitive ability during decision making, either as responsive or remediation actions [26,200]. A generic attack path based on the MITRE attack threat model has been proposed. The generic path will simplify and clarify the TTPs of APT attacks. Consequently, understanding the factors affecting detection efficiency and timeframe will be improved.

These factors specify how the assault is undertaken when launched, in addition to the threat detection efficiency. It is critical as the threats are persistent, and the harm they inflict on a system is more significant when the adversary spends a longer period in the system [166].

5.2.3. Using Game Theory

Traditional cyber security systems concentrate on a one-time assault, a significant shortcoming in combatting persistent, concealed, and complex APT strikes. Nevertheless, if the defender applies AI techniques such as game theory to evaluate the APT assault, establishing the likely attack path and providing an appropriate response architecture are possible [161]. In the context of such long-term and stealthy attacks, it has been recommended that new AI methodologies and relevant analytical tools that intelligently gather threats to enable the detection of APT-type attacks and to guard against them prior to exfiltration are created [116].

Overview of Game Theory

Game theory is a theory that is utilized to analyze problems and make decisions before they occur. It has been used in various domains, including military, political, and social production, and is currently integrated with cyber security and communication. Game theory evaluates all possible assaults on a network from a benefits standpoint and subsequently determines the most efficient and effective defense plan. For instance, game-theoretic approaches have been extensively utilized to describe defender–attacker interactions in networks and process cyber-physical systems using game theory [201].

Conventional cyber security methods are focused on one-time assaults, which leaves a significant gap in dealing with persistent, concealed, and complicated APT attacks [202]. Nevertheless, if the defense used game theory for the APT assault evaluation, it would be able to identify probable attack paths and build a proper protection architecture [161].

APT research has been employing the game theory methodology owing to its potential for investigating the consequences of cyber security attacks and defensive measures in diverse information and communication settings across society. Notwithstanding, a thorough comprehension of the quantification of behavioral impacts and their ramifications for performance, organization, and security remains necessary in a general sense [203]. Game theory explores formal models of strategic interaction among rational and intelligent agents.

The framework presented provides a refined approach to analyzing attributes of APTs, including, but not limited to, their elusive nature and unpredictable behavior. Given the constraints on attacker incentives, defense resource allocations, and attack impacts, it is necessary to consider various factors when analyzing security strategies. Game theory is a suitable approach for formal analysis of strategic interactions based on logical reasoning [204]. Consequently, game-theoretic approaches provide several key advantages, such as proven mathematics, reliable defense, timely action, and distributed solutions. Game theory can methodically and mathematically investigate security choices in proven mathematics.

Researchers have the ability to create defense mechanisms for reliable cyber systems based on the results of the game's analysis. These defense mechanisms are designed to protect these systems from the self-centered behaviors of malicious users. Additionally, game-theoretic strategies assist defenders by allocating limited resources to balance perceived risks by utilizing underlying methods.

Furthermore, the conventional security solution may be adopted more quickly due to the absence of incentives for the people involved. Lastly, most conventional forms of defense are centralized rather than decentralized decision-making structures. Nevertheless, the requirement for a coordinator in an independent system allows for a centralized model in a network security game. Resultantly, appropriate game models will be used to distribute security solutions [205,206].

Game Theory and Cyber Cognitive Situational Awareness (CCSA)

The game theory approach has been presented as a potential strategy for addressing the uncertainty inherent in sophisticated, persistent threats. Its mathematical precision gives security specialists the skills and means to make informed, objective, and transparent decisions [38]. The predictive ability of game theory makes it appropriate for proactive cyber protection. Furthermore, the Nash equilibrium is among the solutions to a cyber security game.

Following a unilateral deviation, no player can raise their payout in a Nash equilibrium profile. Consequently, the defender may adopt the Nash equilibrium profile to estimate the attacker's optimal action. Game theory's predictive ability, cyber deception, mobility, and resilience can serve as the foundation for a comprehensive framework for proactive cyber defense [131]. Moreover, the proposal of a cyber cognitive situational awareness (CCSA) model, such as the Joint Directors of Laboratories (JDL), will be explored further by testing its suitability to detect smartphone attacks [200].

Finally, a smartphone application could be developed to collect the dataset of mobile devices based on the specific static and dynamic features to simulate the APT attack [131].

5.3. The Proposed Conceptual Framework for APT Detection on Smartphone Sensors (FORMAP)

In a broad sense, situation awareness is the perception of environmental elements within an amount of time and space by understanding their meaning and predicting their future status [207]. The sensor data fusion techniques combine the information gathered from several sensors, making the algorithms more accurate in distinguishing between the various activities [208]. Additionally, using data from various distributed sources allows a lower probability of detection errors and higher reliability [209].

The JDL data fusion model is a reference model that outlines the comprehensive procedure of fusing data derived from various sources to understand the observed situation better. This model describes the technical information processes of gaining situation awareness [76].

Algorithms can be used at each stage of the fusion process to combine data and draw conclusions regarding the data based on their context [210]. The JDL model classified the data fusion process into five processing levels: L0 (source preprocessing), LI (object refinement), L2 (situation refinement), L3 (threat refinement) and L4 (process refinement). A conceptual framework has been proposed, as shown in Figure 11, to present a solution to overcome all the challenges relating to the process of APT detection on smartphones.

Data collection: Prior to implementing the five levels of the model, the source stage was applied to collect the data from smartphones. It comprises numerous components, specifically mobile sensing, smartphone applications, APT, and use logging [211]. Various sensors are included in contemporary smartphones, including GPS, Wi-Fi, cameras, microphones, accelerometers, and gyros. Each sensor can sense distinct components of the user context, chosen and set according to the application's requirements. Additionally, it collects information using the mobile application's features [212]. Based on the frequency, duration, and temporal and spatial patterns, determining the usage logs is possible for sensor data, smartphone applications, and APT attacks.

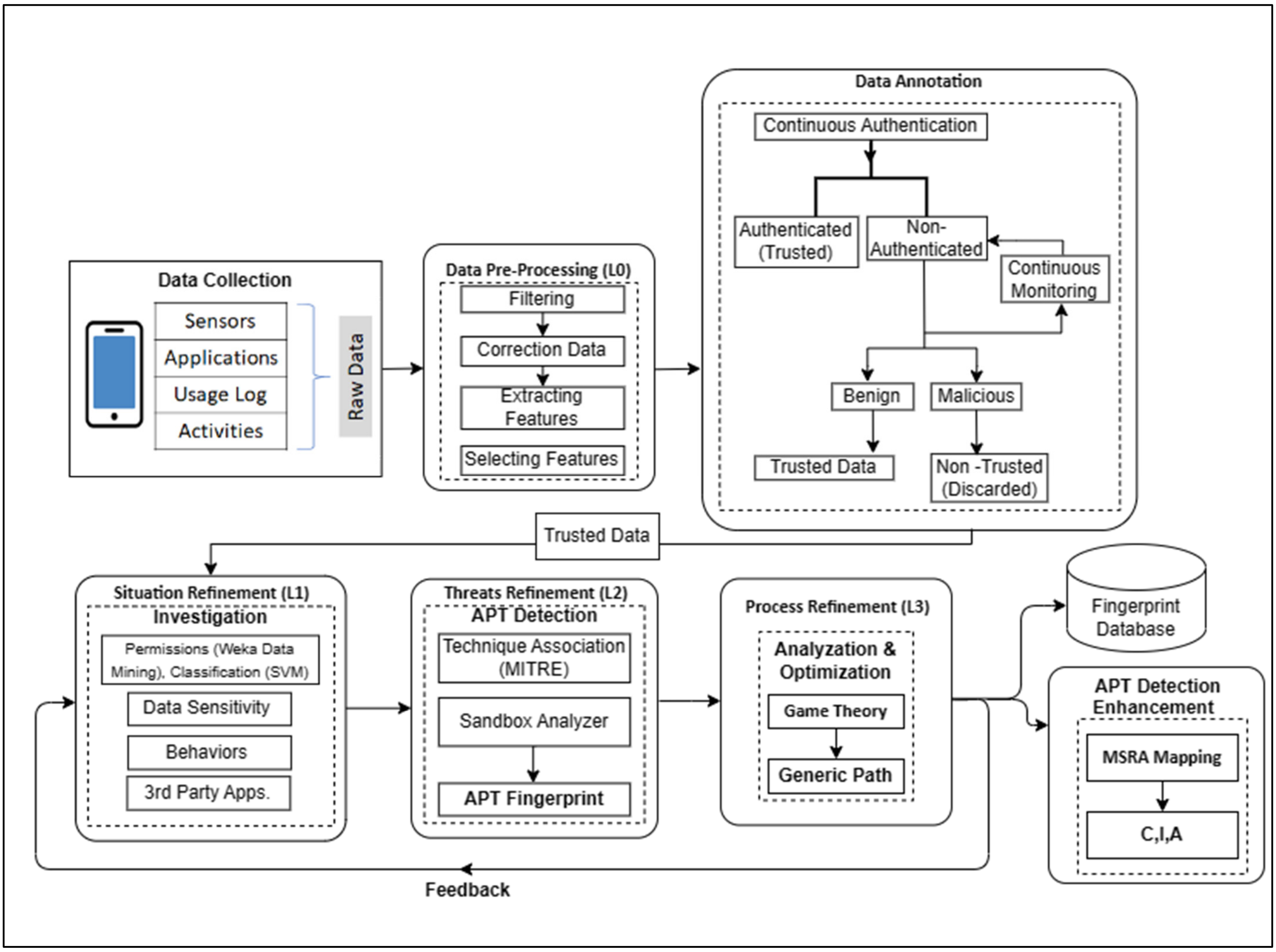

Figure 11. Proposed Conceptual Framework for APT Detection on Smartphone Sensors (FORMAP).

L0: Data preprocessing is the lowest level of the data fusion process. It is considered one of the significant steps in this model and is used to convert raw data into useful and efficient patterns. It includes filtering, correcting the data, and extracting features using Kalman filter algorithms. The data at this stage are refined while being useful to higher-level operations [209]. Notably, data correction procedures should be carried out when collected data fail. Data correction entails using sensor data imputation techniques to estimate missing or inconsistent values [208].

Subsequently, the feature extraction phase is important, where different features are extracted from the raw data. Several features can be extracted using static and dynamic analysis. The features acquired using static analysis rely on command stings, API calls, intentions, and permissions [213]. In order to reduce complexity, eliminate noise, and enhance the model's effectiveness, feature selection chooses only the most crucial features based on their ranking [214].

Data annotation: It has been proposed to adopt the K-means clustering algorithm and continuous authentication for annotating unlabeled raw data to detect trusted and non-trusted data. In a continuous authentication system, the attributes such as networks, connections, applications used, and sensors are monitored while a user uses the mobile device [215]. During the training phase, the vast amounts of sensor data available on mobile devices are used to discover a template or multiple templates for the authorized user. Moreover, the templates are constantly being used in the background for authentication purposes during typical use.

The phone will automatically begin restricting access to the most private apps and features based on how far the user deviates from the device presets. Additionally, the mobile application usage data and timing information can be utilized to identify the precise day and length of time spent in any given application [190].

L1: The situation awareness model has been proposed to select the risky permissions, information sensitivity, and behaviors utilizing the SIGPID model to detect dangerous permissions. Furthermore, it has been suggested that a data-mining technique could be used to extract the risky permission based on a set of association rules for risky permission [216]. Androguard could be used to decompile the applications associated with the dataset to extract permissions from them. It proposes extracting many different types of possible permissions to construct the feature set list.

These permissions included permission rate, type, and the sizes of the applications to undertake static analysis and explicitly grasp each application's behavior. After identifying the list of permissions, filtering, finalizing, and retrieving the essential features will be used to specify the most important permissions to differentiate malicious and benign apps [217]. Permissions are assigned one of the four protection levels, which describe the potential risks they may entail and impose various install-time approval procedures.

These four levels are normal, dangerous, signature, and signature or system. Users are only asked for their express consent for dangerous permissions such as CAMERA, READ_CONTACTS, ACCESS_FINE_LOCATION, and READ_PHONE_STATE [218,219]. Contrarily, vulnerability assessments locate the security gaps that an adversary can penetrate from a distant location and exploit. The primary goals of solutions based on the detection of malicious behavior are the analysis of malicious behavior and preventing malicious apps from being installed on the device [220].

L2: In this threat refinement level, the TTP fingerprint is generated and configured to identify the APT assault during the design stage. The correlation between the virtual sandbox detection and the MITRE framework creates the fingerprint. Sandbox is a type of application emulator which can identify malicious behavior by running the program in a sandbox before bringing it into the real world. Typically, it is used to detect zero-day attacks or modified malware. An APT assault infiltrates a target system utilizing a zero-day vulnerability. Consequently, detection using a virtual sandbox is required for APT defense [221].

In the meantime, MITRE ATT&CK methods and processes analyze cyber artefacts gathered from the network and end system to give behavioral observables for identifying assaults. Analysts can use the framework of TTPs to categorize opposing actions into procedures corresponding to specific strategies and tactics to better understand what an attacker may be trying to accomplish and how to defend against them. While MITRE ATT&CK details various possible attack methods, it fails to suggest how an adversary might combine them to achieve their objectives.

The significance of technique associations lies in their ability to enable analysts to make predictions regarding previously unseen techniques, drawing from those that have been observed in the TTP chain. In the absence of technique associations, an analyst may encounter difficulties in effectively reasoning about adversarial behavior, as the search space grows exponentially with the quantity of techniques provided [70].

L3: In process refinement, AI techniques such as game theory have been proposed throughout the development level due to their capability to investigate the consequences of cyber security attacks and defensive activities in different communication and information contexts within society [203]. Such a condition is achieved by simulating behavioral sequences that maximize the benefits of defenders and mitigating the threat posed by the attackers based on input data and the detection design of the proposed conceptual framework.

Furthermore, it can obtain high precision and performance while offering an efficient model. The evaluation may be accomplished by evaluating the system's accuracy, response time, and efficacy in detecting and mitigating APT attacks on mobile sensors. A dynamic game is proposed in the suggested framework to depict the ongoing interaction between a stealthy attacker and a proactive defender. Multistage games with incomplete information, in which each participant has their own confidential data they do not share with the other, are ideal for capturing sneaky and dishonest behaviors [32].

6. Conclusions

The paper has summarized the most up-to-date user behavior activities and the APT detection mechanism. It has provided a comprehensive overview of AI techniques adopted for APT detection on smartphone sensors. The SLR was carried out on papers published from 2012 to 2023. The activities undertaken by the user on highly vulnerable smartphones have been investigated for potential security attacks. The challenges and problems with adopting AI techniques for APT detection on mobile sensors were also investigated.

The SLR has established that mobile sensors are critical for acquiring, transmitting, and analyzing data within a mobile application. Ultimately, an attacker can exploit several vulnerabilities to breach the mobile sensors. Moreover, APT attacks remain difficult to detect due to the limited focus on human behavioral factors leading to APT, unclear APT attack trails or TTPs, and limited understanding of the attack path that may be followed due to the nature of the APT attack. Furthermore, limited research has used game theory or fuzzy logic as AI techniques for detecting APT attacks on smartphone sensors. Additionally, as the APT attack method is dynamic, identifying the interconnected attack channels formed by APT attackers when vulnerabilities are exploited is significantly complicated.

Regarding the overview analysis and findings relating to the research questions, it is concluded that detecting APTs on smartphone sensors continuously faces several challenges. In order to mitigate these challenges, certain recommendations and solutions have been proposed, such as deriving a conceptual framework to conduct the situation awareness model in line with adopting game theory as an AI technique for APT detection on smartphone sensors. Future studies should focus on employing situation awareness to construct a mathematical framework model. An enhanced and elevated game theory model should be suggested to illustrate how decision making depends on self-adaptation, auto-prediction, and reflection.

Author Contributions: Conceptualization, A.A.A.-K.; Methodology A.A.A.-K. and M.M.S.; software, A.A.A.-K.; validation, A.A.A.-K.; formal analysis, A.A.A.-K.; investigation, A.A.A.-K.; resources, A.A.A.-K.; data curation, A.A.A.-K.; writing— original draft preparation, A.A.A.-K.; writing—review and editing, A.A.A.-K. and M.M.S.; visualization, A.A.A.-K. and M.M.S.; supervision, M.M.S. and M.N.A.K.; project administration, M.M.S.; funding acquisition, M.M.S. and M.N.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme with project Code: FRGS/1/2020/ICT07/USM/02/2.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no known competing financial interest or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Berrada, G.; Cheney, J.; Benabderrahmane, S.; Maxwell, W.; Mookherjee, H.; Theriault, A.; Wright, R. A baseline for unsupervised advanced persistent threat detection in system-level provenance. *Future Gener. Comput. Syst.* **2020**, *108*, 401–413. [CrossRef]
2. Gervasi, O.; Murgante, B.; Misra, S.; Gavrilova, M.L.; Rocha, A.M.A.C.; Torre, C.; Taniar, D.; Apduhan, B.O. Advanced Persistent Threat Mitigation Using Multi Level Security—Access Control Framework. *Lect. Notes Comput. Sci.* **2015**, *9158*, 90–105. [CrossRef]
3. Bann, L.L.; Singh, M.M.; Samsudin, A. Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Comput. Sci.* **2015**, *72*, 129–136. [CrossRef]
4. Powerful Growth: Global Advanced Persistent Threat (APT) Protection Market. Available online: https://www.globenewswire.com/news-release/2021/11/24/2340616/0/en/Powerful-Growth-Global-Advanced-Persistent-Threat-APT-Protection-Market-to-knock-20-290-7-Million-at-a-CAGR-of-20-9-from-2020-to-2027-Research-Dive.html (accessed on 25 December 2022).
5. Ahmad, A.; Webb, J.; Desouza, K.C.; Boorman, J. Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Comput. Secur.* **2019**, *86*, 402–418. [CrossRef]
6. Quintero-Bonilla, S.; del Rey, A.M. A new proposal on the advanced persistent threat: A survey. *Appl. Sci.* **2020**, *10*, 3874. [CrossRef]
7. Advanced Persistent Threat (APT). Available online: https://www.wallarm.com/what/advanced-persistent-threat-apt (accessed on 10 March 2023).
8. Advanced Persistent Threat (APT). Available online: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/#:~:text=Theconsequencesofsuchintrusions,infrastructures(e.g.%2Cdatabasedeletion (accessed on 20 September 2022).
9. Kibona, L.; Ganame, H. Wireless Network Security: Challenges, Threats and Solutions. A Critical Review. *Int. J. Acad. Multidiscip. Res.* **2018**, *2*, 19–27.
10. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *J. Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
11. Al-Kadhimi, A.A.; Singh, M.M.; Jabar, T. Fingerprint for Mobile-Sensor APT Detection Framework (FORMAP) Based on Tactics Techniques and Procedures (TTP) and MITRE. *Lect. Notes Comput. Eng.* **2022**, *835*, 515–533. [CrossRef]
12. Zulkefli, Z.; Mahinderjit Singh, M. Sentient-based Access Control model: A mitigation technique for Advanced Persistent Threats in Smartphones. *J. Inf. Secur. Appl.* **2020**, *51*, 102431. [CrossRef]
13. Remote Access Tool Takes Aim with Android APK Binder. Available online: https://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder (accessed on 12 February 2023).
14. The SmartPhone Who Loved Me. Available online: https://citizenlab.ca/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/ (accessed on 15 November 2022).
15. The Asacub Trojan from Spyware to Banking Malware. Available online: https://securelist.com/the-asacub-trojan-from-spyware-to-banking-malware/73211/ (accessed on 1 January 2023).
16. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1851–1877. [CrossRef]
17. Xing, K.; Li, A.; Jiang, R.; Jia, Y. A review of APT attack detection methods and defense strategies. In Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, China, 27–30 July 2020; No 5. pp. 67–70. [CrossRef]
18. Singh, S.; Sharma, P.K.; Moon, S.Y.; Moon, D.; Park, J.H. A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions. *J. Supercomput.* **2019**, *75*, 4543–4574. [CrossRef]
19. Wang, X.; Liu, Q.; Pan, Z.; Pang, G. APT attack detection algorithm based on spatio-temporal association analysis in industrial network. *J. Ambient Intell. Humaniz. Comput.* **2020**, *1*, e01840. [CrossRef]
20. Blow, F.; Hu, Y.-H.; Hoppa, M. A Study on Vulnerabilities and Threats to Wearable Devices. *J. Colloq. Inf. Syst. Secur. Educ.* **2020**, *7*, 17–27.
21. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
22. Ghafir, I.; Prenosil, V. Advanced Persistent Threat Attack Detection: An Overview. *Int. J. Adv. Comput. Netw. Its Secur.* **2014**, *4*, 50–54.
23. Ghafir, I.; Hammoudeh, M.; Prenosil, V.; Han, L.; Hegarty, R.; Rabie, K.; Aparicio-Navarro, F.J. Detection of advanced persistent threat using machine-learning correlation analysis. *Future Gener. Comput. Syst.* **2018**, *89*, 349–359. [CrossRef]
24. How Artificial Intelligence Will Affect Cybersecurity? Available online: https://geekflare.com/ai-affects-cybersecurity/ (accessed on 2 April 2023).
25. The Use of Artificial Intelligence in Cybersecurity: A Review. Available online: https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity (accessed on 15 March 2023).
26. Park, M.; Han, J.; Oh, H.; Lee, K. Threat Assessment for Android Environment with Connectivity to IoT Devices from the Perspective of Situational Awareness. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1054. [CrossRef]
27. Zimba, A.; Chen, H.; Wang, Z. Bayesian network based weighted APT attack paths modeling in cloud computing. *Future Gener. Comput. Syst.* **2019**, *96*, 525–537. [CrossRef]
28. Flynn, L.; Klieber, W. Smartphone Security. *IEEE Pervasive Computer* **2015**, *14*, 16–21. [CrossRef]

29. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
30. Khalid, M.N.A.; Al-Kadhimi, A.A.; Singh, M.M. Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review. *Mathematics* **2023**, *11*, 1353. [CrossRef]
31. Gopinath, M.; Sethuraman, S.C. A comprehensive survey on deep learning-based malware detection techniques. *Comput. Sci. Rev.* **2023**, *47*, 100529. [CrossRef]
32. Jabar, T.; Mahinderjit Singh, M. Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework. *Sensors* **2022**, *22*, 4662. [CrossRef]
33. Abu Talib, M.; Nasir, Q.; Bou Nassif, A.; Mokhamed, T.; Ahmed, N.; Mahfood, B. APT beaconing detection: A systematic review. *Comput. Secur.* **2022**, *122*, 102875. [CrossRef]
34. Tang, B.H.; Wang, J.F.; Yu, Z.; Chen, B.; Ge, W.; Yu, J.; Lu, T.T. Advanced Persistent Threat intelligent profiling technique: A survey. *Comput. Electr. Eng.* **2022**, *103*, 108261. [CrossRef]
35. Khaleefa, E.J.; Abdulah, D.A. Concept and difficulties of advanced persistent threats (APT): Survey. *Int. J. Nonlinear Anal. Appl.* **2022**, *13*, 2008–6822.
36. Tatam, M.; Shanmugam, B.; Azam, S.; Kannoorpatti, K. A review of threat modelling approaches for APT-style attacks. *Heliyon* **2021**, *7*, e05969. [CrossRef]
37. Bhat, B.A.; Kumar, R. APT: A buzzword and a reality-A bibliometric review of the literature (2010–2020). In Proceedings of the 2021 IEEE 23rd Int Conf on High Performance Computing & Communications; Seventh Int Conf on Data Science & Systems; 19th Int Conf on Smart City; Seventh Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), Haikou, China, 20–22 December 2021; pp. 1972–1979.
38. Kumar, R.; Singh, S.; Kela, R. Analyzing Advanced Persistent Threats Using Game Theory: A Critical Literature Review. *IFIP Adv. Inf. Commun. Technol.* **2022**, *636*, 45–69. [CrossRef]
39. Hussain, S.; Bin Ahmad, M.; Uddin Ghouri, S.S. Advance Persistent Threat—A Systematic Review of Literature and Meta-Analysis of Threat Vectors. *Adv. Intell. Syst. Comput.* **2021**, *1158*, 161–178. [CrossRef]
40. Privacy Assessing Method. Available online: https://www.fireeye.com/blog/threat-research/2013/08/pivy-assessing-damage-and-extracting-intel.html (accessed on 1 January 2023).
41. Spear Phishing Attack. Available online: https://www.fireeye.com/current-threats/reports-by-industry/rpt-spear-phishing-attacks.html (accessed on 12 February 2023).
42. Vukalović, J.; Delija, D. Advanced Persistent Threats—Detection and defense. In Proceedings of the 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 25–29 May 2015; pp. 1324–1330. [CrossRef]
43. Jabar, T.; Singh, M.M.; Al-Kadhimi, A.A. Mobile Advanced Persistent Threat Detection Using Device Behavior (SHOVEL) Framework. In Proceedings of the Eighth International Conference on Computational Science and Technology, Labuan, Malaysia, 28–29 August 2021; Springer: Singapore, 2022; pp. 495–513. [CrossRef]
44. Rass, S.; König, S.; Panaousis, E. Cut-The-Rope: A Game of Stealthy Intrusion. *Lect. Notes Comput. Sci.* **2019**, *11836*, 404–416. [CrossRef]
45. Mahinderjit Singh, M.; Sin Siang, S.; Ying San, O.; Hassain Malim, N.H.A.; Mohd Shariff, A.R. Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model. *Int. J. Mob. Netw. Commun. Telemat.* **2014**, *4*, 4501. [CrossRef]
46. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
47. Aleroud, A.; Zhou, L. Phishing environments, techniques, and countermeasures: A survey. *Comput. Secur.* **2017**, *68*, 160–196. [CrossRef]
48. Symantec. Internet security threat report. *Netw. Secur.* **2016**, *21*, 1–3.
49. Song, L.; Tang, Z.; Li, Z.; Gong, X.; Chen, X.; Fang, D.; Wang, Z. AppIS: Protect android apps against runtime repackaging attacks. In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; pp. 25–32. [CrossRef]
50. Sharma, K.; Gupta, B.B. Mitigation and risk factor analysis of android applications. *Comput. Electr. Eng.* **2018**, *71*, 416–430. [CrossRef]
51. Anatomy of an APT Attack: Step by Step Approach. Anatomy of an APT Attack: Step by Step Approach, [Online]. Available online: https://resources.infosecinstitute.com/topic/anatomy-of-an-apt-attack-step-by-step-approach/ (accessed on 10 February 2023).
52. Hoseini-Tabatabaei, S.A.; Gluhak, A.; Tafazolli, R. A survey on smartphone-based systems for opportunistic user context recognition. *ACM Comput. Surv.* **2013**, *45*, 744. [CrossRef]
53. Zulkefli, Z.; Singh, M.M.; Mohd Shariff, A.R.; Samsudin, A. Typosquat Cyber Crime Attack Detection via Smartphone. *Procedia Comput. Sci.* **2017**, *124*, 6–8. [CrossRef]
54. Android Trojan Found in Targeted Attack. Available online: https://securelist.com/androidtrojan-%0Afound-in-targeted-attack-58/35552/%0A (accessed on 15 April 2023).
55. Cybersecurity Framework. Available online: https://www.nist.gov/industry-impacts/cybersecurity-framework#:~:text=TheFrameworkintegratesindustrystandards,understandingoftheircybersecurityrisks (accessed on 15 November 2022).
56. Cybersecurity Innovation at NIST... and Beyond! Available online: https://www.nccoe.nist.gov/get-involved/attend-events/cybersecurity-innovation-nist-and-beyond (accessed on 25 December 2022).

57. How to Comply in 2020 with the 5 Functions of The NIST Cybersecurity Framework. Available online: https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/ (accessed on 10 February 2023).
58. GPS Weakness Could Enable Mass Smartphone Hacking. Available online: https://www.technologyreview.com/2012/07/26/184742/gps-weakness-could-enable-mass-smartphone-hacking/ (accessed on 15 November 2022).
59. Lonzetta, A.M.; Cope, P.; Campbell, J.; Mohd, B.J.; Hayajneh, T. Security vulnerabilities in bluetooth technology as used in IoT. *J. Sens. Actuator Netw.* **2018**, *7*, 28. [CrossRef]
60. Nahapetian, A. Side-channel attacks on mobile and wearable systems. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016; pp. 243–247. [CrossRef]
61. The Little-Known Ways Mobile Device Sensors Can Be Exploited by Cybercriminals. Available online: https://blog.malwarebytes.com/iot/2019/12/the-little-known-ways-mobile-devicesensors-%0Acan-be-exploited-by-cybercriminals/%0A (accessed on 12 February 2023).
62. Bermejo, C.; Hui, P. Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags. *arXiv* **2017**, arXiv:1705.02081. [CrossRef]
63. Android Phone Vulnerability Gives Apps Access to Your Camera and Microphone without Permission. Available online: https://syncni.com/article/3355/android-phone-vulnerability-givesapps-%0Aaccess-to-your-camera-and-microphone-without-permission#:~:text=Security%0A (accessed on 3 August 2022).
64. Smartphone's Microphone Used for Launching Acoustic Side-Channel Attack. Available online: https://cisomag.eccouncil.org/smartphones-microphone-used-for-launching-acoustic-side-channel-attack-researchers/ (accessed on 12 November 2022).
65. Setting a New Standard for the Long-Term Sustainability of Digital Preservation Services. Available online: https://preservica.com/digital-preservation-sustainability (accessed on 3 January 2023).
66. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G.; Benedetto, L. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hacking Tech.* **2019**, *15*, 277–305. [CrossRef]
67. anda Security. Understanding Cyber-attacks. Part I | 2. Intell. Platf. 2017. Available online: http://resources.pandasecurity.com/enterprise/solutions/ad360/1704-WHITEPAPER-CKC-EN.pdf (accessed on 3 January 2023).
68. Daimi, K. Computer and network security essentials. *Comput. Netw. Secur. Essentials* **2017**, *Canada (Springer International Publishing AG 2018)*, 1–618. [CrossRef]
69. Matthews, T. What Is MITRE ATT&CK: An Explainer | Exabeam. 2019, No June. Available online: https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/ (accessed on 3 January 2023).
70. Al-Shaer, R.; Spring, J.M.; Christou, E. Learning the Associations of MITRE ATT CK Adversarial Techniques. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, June 29–July 1 2020; 1345. [CrossRef]
71. MITRE ATTACK. Available online: https://attack.mitre.org/tactics/mobile/ (accessed on 15 December 2022).
72. MITRE ATT&CK Framework. Available online: https://awakesecurity.com/glossary/mitre-attck-framework (accessed on 15 December 2022).
73. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
74. Sheth, K.; Patel, K.; Shah, H.; Tanwar, S.; Gupta, R.; Kumar, N. A taxonomy of AI techniques for 6G communication networks. *Comput. Commun.* **2020**, *161*, 279–303. [CrossRef]
75. Al-Khassawneh, Y.A. A Review of Artificial Intelligence in Security and Privacy: Research Advances, Applications, Opportunities, and Challenges. *Indones. J. Sci. Technol.* **2023**, *8*, 79–96. [CrossRef]
76. Pahi, T.; Leitner, M.; Skopik, F. Analysis and assessment of situational awareness models for national cyber security centers. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 19–21 February 2017; pp. 334–345. [CrossRef]
77. Endsley, M.R. Toward a theory of situation awareness in dynamic systems. *Situat. Aware.* **2017**, *37*, 9–41. [CrossRef]
78. Nguyen, T.; Lim, C.P.; Nguyen, N.D.; Gordon-Brown, L.; Nahavandi, S. A Review of Situation Awareness Assessment Approaches in Aviation Environments. *IEEE Syst. J.* **2019**, *13*, 3590–3603. [CrossRef]
79. Endsley, M.R. Situation awareness in future autonomous vehicles: Beware of the unexpected. *Adv. Intell. Syst. Comput.* **2019**, *824*, 303–309. [CrossRef]
80. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.T.; Liu, X. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
81. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 879–910. [CrossRef]
82. Budgen, D.; Brereton, P. Performing systematic literature reviews in software engineering. In Proceedings of the 28th International Conference on Software Engineering, New York, NY, USA, 20–28 May 2006; pp. 1051–1052. [CrossRef]
83. Brereton, P.; Kitchenham, B.A.; Budgen, D.; Turner, M.; Khalil, M. Lessons from applying the systematic literature review process within the software engineering domain. *J. Syst. Softw.* **2007**, *80*, 571–583. [CrossRef]
84. Wohlin, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, New York, NY, USA, 13–14 May 2014. [CrossRef]
85. Mahdavi-Hezavehi, S.; Durelli, V.H.S.; Weyns, D.; Avgeriou, P. A systematic literature review on methods that handle multiple quality attributes in architecture-based self-adaptive systems. *Inf. Softw. Technol.* **2017**, *90*, 1–26. [CrossRef]

86. Kable, A.K.; Pich, J.; Maslin-Prothero, S.E. A structured approach to documenting a search strategy for publication: A 12 step guideline for authors. *Nurse Educ. Today* **2012**, *32*, 878–886. [CrossRef] [PubMed]
87. Booth, A. Searching for qualitative research for inclusion in systematic reviews: A structured methodological review. *Syst. Rev.* **2016**, *5*, 1–23. [CrossRef]
88. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Syst. Rev.* **2021**, *10*, 1–11. [CrossRef] [PubMed]
89. Gkioulos, V.; Wangen, G.; Katsikas, S.K.; Kavallieratos, G.; Kotzanikolaou, P. Security awareness of the digital natives. *Informatics* **2017**, *8*, 42. [CrossRef]
90. Gkioulos, V.; Wangen, G.; Katsikas, S.K. User modelling validation over the security awareness of digital natives. *Future Internet* **2017**, *9*, 32. [CrossRef]
91. Oleg, M.; Ekaterina, P. Security and Privacy Risk Estimation for Personal Data Stored on Mobile Devices. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 730–736.
92. Govindaraj, J.; Verma, R.; Gupta, G. Chapter 6—Analyzing mobile device ads. In Proceedings of the 12th IFIP WG 11.9 International Conference, New Delhi, India, 4–6 January 2016; pp. 107–126. [CrossRef]
93. Shah, P.; Agarwal, A. Cybersecurity behaviour of smartphone users in India: An empirical analysis. *Inf. Comput. Secur.* **2020**, *28*, 293–318. [CrossRef]
94. Downer, K.; Bhattacharya, M. BYOD Security: A Study of Human Dimensions. *Informatics* **2022**, *9*, 16. [CrossRef]
95. Costantino, G.; Matteucci, I. CANDY CREAM—Hacking infotainment android systems to command instrument cluster via can data frame. In Proceedings of the 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 1–3 August 2019; pp. 476–481. [CrossRef]
96. Mehrnezhad, M.; Toreini, E.; Shahandashti, S.F.; Hao, F. TouchSignatures: Identification of user touch actions and PINs based on mobile sensor data via JavaScript. *J. Inf. Secur. Appl.* **2016**, *26*, 23–38. [CrossRef]
97. Wang, C.; Wang, Y.; Chen, Y.; Liu, H.; Liu, J. User authentication on mobile devices: Approaches, threats and trends. *Comput. Netw.* **2020**, *170*, 107118. [CrossRef]
98. Mehrnezhad, M.; Toreini, E.; Shahandashti, S.F.; Hao, F. Stealing PINs via mobile sensors: Actual risk versus user perception. *Int. J. Inf. Secur.* **2018**, *17*, 291–313. [CrossRef] [PubMed]
99. Lee, S.; Ryu, S. Adlib: Analyzer for mobile ad platform libraries. In Proceedings of the ISSTA 2019: Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, Beijing, China, 15–19 July 2019; pp. 262–272. [CrossRef]
100. Zhou, L.; Kang, Y.; Zhang, D.; Lai, J. Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones. *Decis. Support Syst.* **2016**, *92*, 14–24. [CrossRef]
101. Liu, H.; Ning, H.; Yue, Y.; Wan, Y.; Yang, L.T. Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices. *Future Gener. Comput. Syst.* **2018**, *78*, 976–986. [CrossRef]
102. Jalbani, K.B.; Yousaf, M.; Sarfraz, M.S.; Jamili Oskouei, R.; Hussain, A.; Memon, Z. Poor Coding Leads to DoS Attack and Security Issues in Web Applications for Sensors. *Secur. Commun. Netw.* **2021**, *2021*, 5523806. [CrossRef]
103. Stirparo, P.; Fovino, I.N.; Taddeo, M.; Kounelis, I. In-memory credentials robbery on android phones. In Proceedings of the World Congress on Internet Security (WorldCIS-2013), London, UK, 9–12 December 2013; pp. 88–93. [CrossRef]
104. Perumal, S.; Kola Sujatha, P. Stacking Ensemble-based XSS Attack Detection Strategy Using Classification Algorithms. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 8–10 July 2021; pp. 897–901. [CrossRef]
105. Software Classification. Available online: https://www.educba.com/software-classification/ (accessed on 25 February 2023).
106. Lero, A.R.S.; Lero, J.B.; Gear, A.L. Privacy and security analysis of cryptocurrency mobile applications. In Proceedings of the 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2–3 March 2019; pp. 1–6. [CrossRef]
107. Tu, Z.; Yuan, Y. Understanding user behaviour in coping with security threats of mobile device loss and theft. In Proceedings of the 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2014; p. 12.
108. Morrow, B. BYOD security challenges: Control and protect your most sensitive data. *Netw. Secur.* **2012**, *2012*, 5–8. [CrossRef]
109. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef]
110. Gervasi, O.; Murgante, B.; Misra, S.; Gavrilova, M.L.; Rocha, A.M.A.C.; Torre, C.; Taniar, D.; Apduhan, B.O. *Computational Science and Its Applications, Proceedings of the ICCSA 2015: 15th International Conference, Banff, AB, Canada, 22–25 June 2015*; Lecture Notes in Computer Science; ICCSA: Banff, AB, Canada, 2015; Part IV, Volume 9158, pp. 90–105. [CrossRef]
111. Wang, C.; Anand, S.A.; Liu, J.; Walker, P.; Chen, Y.; Saxena, N. Defeating hidden audio channel attacks on voice assistants via audio-induced surface vibrations. In Proceedings of the ACSAC '19, 35th Annual Computer Security Applications Conference, San Juan, PR, USA, 9–13 December 2019; pp. 42–56. [CrossRef]
112. Park, S.; Shaik, A.; Borgaonkar, R.; Seifert, J.P. White rabbit in mobile: Effect of unsecured clock source in smartphones. In SPSM '16: Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices, Vienna, Austria, 24 October 2016; 16, pp. 13–21. [CrossRef]
113. Seo, S.; Yim, K.; You, I. Mobile Malware Threats and Defenses. *IFIP Int. Fed. Inf. Process.* **2012**, *1*, 516–524.

114. Bakar, A.A.; Singh, M.M.; Shariff, A.R.M. A privacy preservation quality of service (Qos) model for data exposure in android smartphone usage. *Sensors* **2021**, *21*, 1667. [CrossRef]
115. Sikder, A.K.; Petracca, G.; Aksu, H.; Jaeger, T.; Uluagac, A.S. A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1125–1159. [CrossRef]
116. Abdullayeva, F.J. Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. *Array* **2021**, *10*, 100067. [CrossRef]
117. Vance, A. Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing. In Proceedings of the 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology, Kharkov, Ukraine, 14–17 October 2014; pp. 173–176. [CrossRef]
118. Yang, J.; Zhang, Q.; Jiang, X.; Chen, S.; Yang, F. Poirot: Causal Correlation Aided Semantic Analysis for Advanced Persistent Threat Detection. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 3546–3563. [CrossRef]
119. Ahmed, Y.; Asyhari, A.T.; Rahman, M.A. A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. *Comput. Mater. Contin.* **2021**, *67*, 2497–2513. [CrossRef]
120. Panahnejad, M.; Mirabi, M. APT-Dt-KC: Advanced persistent threat detection based on kill-chain model. *J. Supercomput.* **2022**, *4*, 8644–8677. [CrossRef]
121. Maccari, M.; Polzonetti, A.; Sagratella, M. *Detection: Definition of New Model to Reveal Advanced Persistent Threat*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 881. [CrossRef]
122. Siddiqui, S.; Khan, M.S.; Ferens, K.; Kinsner, W. Detecting advanced persistent threats using fractal dimension based machine learning classification. In Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics, New Orleans, LA, USA, 11 March 1016; pp. 64–69. [CrossRef]
123. Wang, Y.; Wang, Y.; Liu, J.; Huang, Z. A network gene-based framework for detecting advanced persistent threats. In Proceedings of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, China, 8–10 November 2014; pp. 97–102. [CrossRef]
124. McLaren, P.; Russell, G.; Buchanan, B. Mining malware command and control traces. In Proceedings of the 2017 Computing Conference, London, UK, 18–20 July 2017; pp. 788–794. [CrossRef]
125. Do Xuan, C.; Dao, M.H.; Nguyen, H.D. APT attack detection based on flow network analysis techniques using deep learning. *J. Intell. Fuzzy Syst.* **2020**, *39*, 4785–4801. [CrossRef]
126. Li, J.; Zhai, L.; Zhang, X.; Quan, D. Research of android malware detection based on network traffic monitoring. In Proceedings of the 2014 9th IEEE Conference on Industrial Electronics and Applications, Hangzhou, China, 9–11 June 2014; No 2011; pp. 1739–1744. [CrossRef]
127. Xuan, C.D. Detecting APT attacks based on network traffic using machine learning. *J. Web Eng.* **2021**, *20*, 171–190. [CrossRef]
128. Lin, S.; Li, Y.; Du, X. Study and research of APT detection technology based on big data processing architecture. In Proceedings of the 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication, Beijing, China, 14–16 May 2015; No 2012; pp. 313–316. [CrossRef]
129. Cheng, X.; Zhang, J.; Chen, B. *Correlate the Advanced Persistent Threat Alerts and Logs for Cyber Situation Comprehension*; Springer: Singapore, 2019. [CrossRef]
130. Cheng, X.; Zhang, J.; Chen, B. Cyber Situation Comprehension for IoT Systems based on APT Alerts and Logs Correlation. *Sensors* **2019**, *19*, 4045. [CrossRef]
131. Cho, D.X.; Nam, H.H. A method of monitoring and detecting APT attacks based on unknown domains. *Procedia Comput. Sci.* **2019**, *150*, 316–323. [CrossRef]
132. Cheng, X.; Luo, Q.; Pan, Y.; Li, Z.; Zhang, J.; Chen, B. Predicting the APT for Cyber Situation Comprehension in 5G-Enabled IoT Scenarios Based on Differentially Private Federated Learning. *Secur. Commun. Netw.* **2021**, *2021*, 8814068. [CrossRef]
133. Al-Saraireh, J.; Masarweh, A. A novel approach for detecting advanced persistent threats. *Egypt. Inform. J.* **2022**, *23*, 45–55. [CrossRef]
134. Do, X.C.; Huong, D.T.; Nguyen, T. A novel intelligent cognitive computing-based APT malware detection for Endpoint systems. *J. Intell. Fuzzy Syst.* **2022**, *43*, 3527–3547. [CrossRef]
135. Sharma, A.; Gupta, B.B.; Singh, A.K.; Saraswat, V.K. Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense. *Comput. Secur.* **2022**, *115*, 102627. [CrossRef]
136. Xiong, C.; Zhu, T.; Dong, W.; Ruan, L.; Yang, R.; Cheng, Y.; Chen, Y.; Cheng, S.; Chen, X. Conan: A Practical Real-Time APT Detection System with High Accuracy and Efficiency. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 551–565. [CrossRef]
137. Park, S.H.; Yun, S.W.; Jeon, S.E.; Park, N.E.; Shim, H.Y.; Lee, Y.R.; Lee, S.J.; Park, T.R.; Shin, N.Y.; Kang, M.J.; et al. Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection. *IEEE Access* **2022**, *10*, 20259–20269. [CrossRef]
138. Zimba, A.; Chen, H.; Wang, Z.; Chishimba, M. Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. *Future Gener. Comput. Syst.* **2020**, *106*, 501–517. [CrossRef]
139. Alsanad, A.; Altuwaijri, S. Advanced Persistent Threat Attack Detection using Clustering Algorithms. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 640–649. [CrossRef]

140. Neuschmied, H.; Winter, M.; Stojanovi, B.; Hofer-schmitz, K.; Boži, J.; Kleb, U. applied sciences APT-Attack Detection Based on Multi-Stage Autoencoders. *Appl. Sci.* **2022**, 1–18.
141. Chuan, B.L.J.; Singh, M.M.; Shariff, A.R.M. APTGuard: Advanced persistent threat (APT) detections and predictions using android smartphone. *Lect. Notes Electr. Eng.* **2019**, *481*, 545–555. [CrossRef]
142. Xiang, Z.; Guo, D.; Li, Q. Detecting mobile advanced persistent threats based on large-scale DNS logs. *Comput. Secur.* **2020**, *96*, 101933. [CrossRef]
143. Niu, W.; Zhang, X.; Yang, G.; Zhu, J.; Ren, Z. Identifying APT malware domain based on mobile DNS logging. *Math. Probl. Eng.* **2017**, *2017*, 6953. [CrossRef]
144. Anto, A.; Rao, R.S.; Pais, A.R. *Kernel Modification APT Attack Detection in Android*; Springer: Singapore; pp. 236–249. [CrossRef]
145. Isotalo, L. 5G Slicing as a tool to test user equipment against advanced persistent threats. *Lect. Notes Comput. Sci.* **2017**, *10394*, 595–603. [CrossRef]
146. Roseline, S.A.; Geetha, S. Android Malware Detection and Classification using LOFO Feature Selection and Tree-based Models. *J. Phys. Conf. Ser.* **2021**, *1911*, e012031. [CrossRef]
147. Fratantonio, Y.; Bianchi, A.; Robertson, W.; Kirda, E.; Kruegel, C.; Vigna, G. TriggerScope: Towards Detecting Logic Bombs in Android Applications. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 377–396. [CrossRef]
148. Alshahrani, H.; Mansourt, H.; Thorn, S.; Alshehri, A.; Alzahrani, A.; Fu, H. DDefender: Android application threat detection using static and dynamic analysis. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018; pp. 1–6. [CrossRef]
149. Li, J.J.; Abbate, P.; Vega, B. Detecting Security Threats Using Mobile Devices. In Proceedings of the 2015 IEEE International Conference on Software Quality, Reliability and Security-Companion, Vancouver, BC, Canada, 3–5 August 2015; pp. 40–45. [CrossRef]
150. Kim, K.; Shin, Y.; Lee, J.; Lee, K. Automatically attributing mobile threat actors by vectorized ATT&CK matrix and paired indicator. *Sensors* **2021**, *21*, 6522. [CrossRef]
151. Almiani, M.; AbuGhazleh, A.; Jararweh, Y.; Razaque, A. DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network. *Int. J. Mach. Learn. Cybern.* **2021**, *1*, 1323. [CrossRef]
152. Toutsop, O.; Harvey, P.; Kornegay, K. Monitoring and detection time optimization of man in the middle attacks using machine learning. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, USA, 13–15 October 2020. [CrossRef]
153. Kim, S.; Hwang, C.; Lee, T. Anomaly based unknown intrusion detection in endpoint environments. *Electronics* **2020**, *9*, 1022. [CrossRef]
154. Javed, S.H.; Bin Ahmad, M.; Asif, M.; Almotiri, S.H.; Masood, K.; Al Ghamdi, M.A. An Intelligent System to Detect Advanced Persistent Threats in Industrial Internet of Things (I-IoT). *Electronics* **2022**, *11*, 742. [CrossRef]
155. Tian, W.; Du, M.; Ji, X.; Liu, G.; Dai, Y.; Han, Z. Honeypot Detection Strategy against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game. *IEEE Internet Things J.* **2021**, *8*, 17372–17381. [CrossRef]
156. Gupta, B.B.; Yadav, K.; Razzak, I.; Psannis, K.; Castiglione, A.; Chang, X. A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. *Comput. Commun.* **2021**, *175*, 47–57. [CrossRef]
157. Mao, J.; Bian, J.; Tian, W.; Zhu, S.; Wei, T.; Li, A.; Liang, Z. Detecting Phishing Websites via Aggregation Analysis of Page Layouts. *Procedia Comput. Sci.* **2018**, *129*, 224–230. [CrossRef]
158. Mahdavifar, S.; Ghorbani, A.A. DeNNeS: Deep embedded neural network expert system for detecting cyber attacks. *Neural Comput. Appl.* **2020**, *32*, 14753–14780. [CrossRef]
159. Xiao, L.; Xu, D.; Mandayam, N.B.; Poor, H.V. Attacker-Centric View of a Detection Game against Advanced Persistent Threats. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2512–2523. [CrossRef]
160. Huang, L.; Zhu, Q. A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. *Comput. Secur.* **2020**, *89*, 1660. [CrossRef]
161. Su, Y. Research on APT attack based on game model. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (IT-NEC), Chongqing, China, 12–14 June 2020; pp. 295–299. [CrossRef]
162. Moothedath, S.; Sahabandu, D.; Allen, J.; Clark, A.; Bushnell, L.; Lee, W.; Poovendran, R. A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multistage Advanced Persistent Threats. *IEEE Trans. Automat. Contr.* **2020**, *65*, 5248–5263. [CrossRef]
163. Abass, A.A.A.; Xiao, L.; Mandayam, N.B.; Gajic, Z. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access* **2017**, *5*, 8482–8491. [CrossRef]
164. Wan, Z.; Cho, J.H.; Zhu, M.; Anwar, A.H.; Kamhoua, C.A.; Singh, M.P. Foureye: Defensive Deception Against Advanced Persistent Threats via Hypergame Theory. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 112–129. [CrossRef]
165. Zhu, Q.; Rass, S. On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats. *IEEE Access* **2018**, *6*, 13958–13971. [CrossRef]
166. Sahabandu, D.; Allen, J.; Moothedath, S.; Bushnell, L.; Lee, W.; Poovendran, R. Quickest detection of advanced persistent threats: A semi-markov game approach. In Proceedings of the 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), Sydney, Australia, 21–25 April 2020; pp. 9–19. [CrossRef]

167. Feng, S.; Xiong, Z.; Niyato, D.; Wang, P. Dynamic Resource Management to Defend against Advanced Persistent Threats in Fog Computing: A Game Theoretic Approach. *IEEE Trans. Cloud Comput.* **2021**, *9*, 995–1007. [CrossRef]
168. Feng, S.; Xiong, Z.; Niyato, D.; Wang, P.; Leshem, A. Evolving Risk Management Against Advanced Persistent Threats in Fog Computing. In Proceedings of the 2018 IEEE 7th International Conference on Cloud Networking (CloudNet), Tokyo, Japan, 22–24 October 2018; 4082187, pp. 1–6. [CrossRef]
169. De Campos Souza, P.V.; Rezende, T.S.; Guimaraes, A.J.; Araujo, V.S.; Batista, L.O.; Da Silva, G.A.; Silva Araujo, V.J. Evolving fuzzy neural networks to aid in the construction of systems specialists in cyber attacks. *J. Intell. Fuzzy Syst.* **2019**, *36*, 6743–6763. [CrossRef]
170. Almomani, A.; Wan, T.; Altaher, A.; Manasrah, A.; Almomani, E.; Anbar, M.; Alomari, E.; Ramadass, S. Evolving Fuzzy Neural Network for Phishing Emails Detection National Advanced IPv6 Centre (NAV6). *J. Comput. Sci.* **2012**, *8*, 1099–1107.
171. Rahman, Z.; Yi, X.; Khalil, I. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet Things J.* **2022**, *3*, 47186. [CrossRef]
172. Do Xuan, C.; Huong, D. A new approach for APT malware detection based on deep graph network for endpoint systems. *Appl. Intell.* **2022**, *52*, 14005–14024. [CrossRef]
173. Do, X.C.; Huong, D.T.; Duong, D. New approach for APT malware detection on the workstation based on process profile. *J. Intell. Fuzzy Syst.* **2022**, *43*, 4815–4834. [CrossRef]
174. Wu, Q.; Li, Q.; Guo, D.; Meng, X. Exploring the vulnerability in the inference phase of advanced persistent threats. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 417. [CrossRef]
175. Do Xuan, C.; Duong, D. Optimization of APT attack detection based on a model combining attention and deep learning. *J. Intell. Fuzzy Syst.* **2022**, *42*, 4135–4151. [CrossRef]
176. Niu, W.; Zhou, J.; Zhao, Y.; Zhang, X.; Peng, Y.; Huang, C. Uncovering APT malware traffic using deep learning combined with time sequence and association analysis. *Comput. Secur.* **2022**, *120*, 102809. [CrossRef]
177. Li, H.; Wu, J.; Xu, H.; Li, G.; Guizani, M. Explainable Intelligence-Driven Defense Mechanism Against Advanced Persistent Threats: A Joint Edge Game and AI Approach. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 757–775. [CrossRef]
178. Moothedath, S.; Sahabandu, D.; Allen, J.; Clark, A.; Bushnell, L.; Lee, W.; Poovendran, R. Dynamic Information Flow Tracking for Detection of Advanced Persistent Threats: A Stochastic Game Approach. *arXiv* **2020**, arXiv:2006.12327. [CrossRef]
179. Bi, J.; He, S.; Luo, F.; Meng, W.; Ji, L.; Huang, D.W. Defense of Advanced Persistent Threat on Industrial Internet of Things with Lateral Movement Modelling. *IEEE Trans. Ind. Inform.* **2022**, *32*, 31406. [CrossRef]
180. Rubio, J.E.; Alcaraz, C.; Lopez, J. Game Theory-Based Approach for Defense Against APTs. *Lect. Notes Comput. Sci.* **2020**, *12147*, 297–320. [CrossRef]
181. Nisioti, A.; Loukas, G.; Rass, S.; Panaousis, E. Game-Theoretic Decision Support for Cyber Forensic Investigations. *Sensors* **2021**, *21*, 5300.
182. Martín, A.; Lara-Cabrera, R.; Camacho, D. Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset. *Inf. Fusion* **2019**, *52*, 128–142. [CrossRef]
183. Javed, A.R.; Rehman, S.U.; Khan, M.U.; Alazab, M.; Khan, H.U. Betalogger: Smartphone Sensor-based Side-channel Attack Detection and Text Inference Using Language Modeling and Dense MultiLayer Neural Network. *ACM Trans. Asian Low-Resour. Lang. Inf. Process.* **2021**, *20*, 392. [CrossRef]
184. Imtiaz, S.I.; ur Rehman, S.; Javed, A.R.; Jalil, Z.; Liu, X.; Alnumay, W.S. DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network. *Future Gener. Comput. Syst.* **2021**, *115*, 844–856. [CrossRef]
185. Fernandez Maimo, L.; Perales Gomez, A.L.; Garcia Clemente, F.J.; Gil Perez, M.; Martinez Perez, G. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *IEEE Access* **2018**, *6*, 7700–7712. [CrossRef]
186. Taheri, R.; Shojafar, M.; Alazab, M.; Tafazolli, R. FED-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT. *IEEE Trans. Ind. Inform.* **2020**, *3*, 3458. [CrossRef]
187. Hussain, B.; Du, Q.; Sun, B.; Han, Z. Deep Learning-Based DDoS-Attack Detection for Cyber-Physical System over 5G Network. IEEE Trans. *Ind. Inform.* **2021**, *17*, 860–870. [CrossRef]
188. Waqas, M.; Tu, S.; Wan, J.; Mir, T.; Alasmary, H.; Abbas, G. Defense scheme against advanced persistent threats in mobile fog computing security. *Comput. Netw.* **2023**, *221*, 109519. [CrossRef]
189. Correia, M.J.; Matos, F. The impact of artificial intelligence on innovation management: A literature review. *Proc. Eur. Conf. Innov. Entrep. ECIE* **2021**, *1*, 222–230. [CrossRef]
190. Mahbub, U.; Komulainen, J.; Ferreira, D.; Chellappa, R. Continuous authentication of smartphones based on application usage. *IEEE Trans. Biom. Behav. Identity Sci.* **2019**, *1*, 165–180. [CrossRef]
191. Senanayake, J.; Kalutarage, H.; Al-Kadri, M.O. Android Mobile Malware Detection Using Machine Learning. *Electronics* **2021**, *10*, 1606.
192. Ching, K.W.; Singh, M.M. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 19–30. [CrossRef]
193. Mahinderjit, M.; Wai, C.; Zulkefli, Z. Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 53–62. [CrossRef]
194. How Cognitive Bias Leads to Reasoning Errors in Cybersecurity. Available online: https://www.forcepoint.com/blog/insights/how-cognitive-bias-leads-reasoning-errors-cybersecurity (accessed on 10 March 2023).

195. Rass, S.; König, S.; Schauer, S. Defending against Advanced Persistent Threats Using Game-Theory. *PLOS ONE* **2017**, *12*, e0168675. [CrossRef]
196. Artificial Intelligence for Security: Real Limitations. Available online: https://blog.morphisec.com/artificial-intelligence-for-security-real-limitations (accessed on 15 December 2022).
197. The Promise and Challenges of AI and Machine Learning for Cybersecurity. Available online: https://www.cpomagazine.com/cyber-security/the-promise-and-challenges-of-ai-and-machine-learning-for-cybersecurity/ (accessed on 2 April 2023).
198. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. A situation awareness model for information security risk management. *Comput. Secur.* **2014**, *44*, 1–15. [CrossRef]
199. What Is Situational Awareness. Available online: https://www.coolfiresolutions.com/blog/what-is-situational-awareness/%0A%0A (accessed on 7 January 2023).
200. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
201. Zhu, Q.; Başar, T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Syst.* **2015**, *35*, 46–65. [CrossRef]
202. Feng, X.; Zheng, Z.; Cansever, D.; Swami, A.; Mohapatra, P. Stealthy attacks with insider information: A game theoretic model with asymmetric feedback. In Proceedings of the MILCOM 2016—2016 IEEE Military Communications Conference, Baltimore, MD, USA, 1–3 November 2016; pp. 277–282. [CrossRef]
203. Lee, S.; Kim, S.; Choi, K.; Shon, T. Game theory-based Security Vulnerability Quantification for Social Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 752–760. [CrossRef]
204. Van Dijk, M.; Juels, A.; Oprea, A.; Rivest, R.L. FlipIt: The game of "stealthy takeover". *J. Cryptol.* **2013**, *26*, 655–713. [CrossRef]
205. Ho, E.; Rajagopalan, A.; Skvortsov, A.; Arulampalam, S.; Piraveenan, M. Game Theory in Defence Applications: A Review. *Sensors* **2022**, *22*, 1032. [CrossRef]
206. Do, C.T.; Tran, N.H.; Hong, C.; Kamhoua, C.A.; Kwiat, K.A.; Blasch, E.; Ren, S.; Pissinou, N.; Iyengar, S.S. Game theory for cyber security and privacy. *ACM Comput. Surv.* **2017**, *50*, 30–37. [CrossRef]
207. Valiente, M.; Machín, R.; García-barriocanal, E. Preface INISET 2011. *Lect. Notes Bus. Inf. Process.* **2011**, *83*, 269. [CrossRef]
208. Pires, I.M.; Garcia, N.M.; Pombo, N.; Flórez-Revuelta, F. From data acquisition to data fusion: A comprehensive review and a roadmap for the identification of activities of daily living using mobile devices. *Sensors* **2016**, *16*, 184. [CrossRef]
209. Castanedo, F. A review of data fusion techniques. *Sci. World J.* **2013**, *2013*, 4504. [CrossRef]
210. Giacobe, N.A. Application of the JDL data fusion process model for cyber security. *Multisens. Multisource Inf. Fusion Archit. Algorithms Appl.* **2010**, *7710*, 77100R. [CrossRef]
211. Natarajasivan, D.; Govindarajan, M. An Overview on Mobile Data Mining. *Int. J. Comput. Appl.* **2014**, *99*, 11–14. [CrossRef]
212. Rendall, K.; Nisioti, A.; Mylonas, A. Towards a multi-layered phishing detection. *Sensors* **2020**, *20*, 4540. [CrossRef]
213. Dhalaria, M.; Gandotra, E. CSForest: An approach for imbalanced family classification of android malicious applications. *Int. J. Inf. Technol.* **2021**, *13*, 1059–1071. [CrossRef]
214. Ismael, A.A.; Jayabalan, M.; Al-Jumeily, D. A study on human activity recognition using smartphone. *J. Adv. Res. Dyn. Control Syst.* **2020**, *12*, 795–803. [CrossRef]
215. Alqarni, M.A.; Chauhdary, S.H.; Malik, M.N.; Ehatisham-ul-Haq, M.; Azam, M.A. Identifying smartphone users based on how they interact with their phones. *Hum.-Cent. Comput. Inf. Sci.* **2020**, *10*, 7. [CrossRef]
216. Kumar, R.; Zhang, X.; Wang, W.; Khan, R.U.; Kumar, J.; Sharif, A. A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features. *IEEE Access* **2019**, *7*, 64411–64430. [CrossRef]
217. Akbar, F.; Hussain, M.; Mumtaz, R.; Riaz, Q.; Wahab, A.W.A.; Jung, K.H. Permissions-Based Detection of Android Malware Using Machine Learning. *Symmetry* **2022**, *14*, 718. [CrossRef]
218. Xu, W.; Zhang, F.; Zhu, S. Permlyzer: Analyzing permission usage in Android applications. 2013 IEEE 24th International Symposium on Software Reliability Engineering (ISSRE), Pasadena, CA, USA, 4–7 November 2017; pp. 400–410. [CrossRef]
219. Gashi, E.; Tafa, Z. Permission-based Privacy Analysis for Android Applications. *Int. J. Bus. Technol.* **2018**, *6*, 1–11. [CrossRef]
220. Acharya, S.; Rawat, U.; Bhatnagar, R. A Comprehensive Review of Android Security: Threats, Vulnerabilities, Malware Detection, and Analysis. *Secur. Commun. Netw.* **2022**, *2022*, 5917. [CrossRef]
221. Moon, D.; Im, H.; Lee, J.D.; Park, J.H. MLDS: Multi-layer defense system for preventing advanced persistent threats. *Symmetry* **2014**, *6*, 997–1010. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.