International Journal for Multidisciplinary Research (IJFMR)

E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Comprehensive Analysis to Detect Mobile Malware Using Multiple Techniques

Divya Sharma[1], Jasvir Singh[2]

[1,2]Department of Computer Science & Engineering, Punjabi University, Patiala

Abstract

Mobile devices have end up integral elements of our each day lives, storing great quantities of private and sensitive data. However, this convenience comes with inherent dangers, as cybercriminals increasingly more goal cellular devices for malicious sports consisting of stealing personal statistics, disrupting operations, and compromising the working machine. Various sorts of cellular malware, together with Remote Access Tools (RATs), Bank Trojans, Ransomware, Cryptomining Malware, and Advertising Click Fraud, pose sizable threats to users' privateness and protection. Detecting and mitigating cell malware is essential in safeguarding customers' gadgets and statistics. This paper systematically examines and surveys cellular malware detection strategies, specializing in traditional and superior strategies. Traditional detection methods encompass signature-based detection, conduct-primarily based detection, and permission analysis, while superior techniques embody gadget studying-based detection and anomaly detection. Each approach has its strengths and obstacles, emphasizing the significance of using a mixture of strategies for complete safety. The paper reviews relevant literature to research the effectiveness of different detection techniques and their packages in actual-global situations. It discusses the evolution of malware detection methodologies, highlighting advancements which include mobile botnet type, dynamic anomaly-based totally detection, and characteristic-based adverse attacks on device getting to know classifiers. Additionally, the paper explores the demanding situations confronted via cutting-edge detection techniques and proposes avenues for future research to address those obstacles. By presenting a comprehensive evaluation of cell malware detection strategies, this thesis contributes to the advancement of studies in cybersecurity and aids in the improvement of greater strong and green detection mechanisms to combat evolving threats in the cellular surroundings.

Keywords: Mobile Malware, Signature-Based Detection, Behavior Based Detection, Machine Learning Based Detection, Anomaly Based Detection.

1. INTRODUCTION

The smartphones or the mobile devices we carry stores alot of information about the financial transactions, our access to social media and many other personal information about us. However, because of this comfort the mobile devices are targeted for malicious activities. Mobile malware is designed to infect the mobile devices in order to steal the personal information, interfere with normal operations, harm the operating system of the mobile etc. Virus, Worms, Trojan, Botnets and many more are few types of malware. Cybercriminals practice various ways to infect or disrupt the mobile devices, some most common types of mobile malwares are RATs, Bank Trojans, Ransomware, Cryptomining Malware, Advertising Click Fraud. RATs are shortened for Remote Access Tool, it offers wide access to data from infected victims devices. It can access information like web browsing history, installed applications, sms data, call history and many more. RATs can also be used to log GPS data, send sms and enable device cameras [1]. A form of malware known as a bank trojan tries to obtain financial login and password details from users who conduct their banking activities, such as money transfers and bill payments, via mobile devices. These trojans are frequently presented as genuine applications. Malware that locks users out of their devices and demands a "ransom" payment, usually in the form of untraceable Bitcoin, is known as ransomware. The victim receives access codes to unlock their mobile device once they pay the ransom. Attackers can generate bitcoin by surreptitiously carrying out calculations on a victim's device through the use of cryptomining malware [2]. Trojan code, which is concealed in apps that appear authentic, is frequently used for cryptocurrency mining. Malware known as "Advertising Click Fraud" enables an attacker to take control of a device and use phony ad clicks to make money. Some common ways by which the attackers rely on to distribute their malicious code are Mobile phishing and spoofing, jailbreaking or rooting, drive-by downloads, trojanized apps, malvertising, infected document and many more [3].

2. DETECTION TECHNIQUES

The mobile devices carries each and every information about its user, so these devices are targeted by the cybercriminals to gain unauthorized access to the user's device. Mobile malware detection techniques are essential for many reasons such as the increase in the use of mobile devices has made these devices profitable for the cybercriminals who seek to steal the personal or sensitive information or exploit the vulnerabilities [4]. The mobile malware detection techniques are classified into two categories traditional detection techniques and advanced detection techniques. As shown in figure 1 the traditional detection techniques are classified into signature-based detection, behavior-based detection, permission analysis, static analysis and many more. The advanced detection techniques include machine learning-based detection, anomaly detection, dynamic analysis, root cause analysis and many more. In this paper we are discussing about the signature-based detection and behavior-based detection, machine learning-based detection and anomaly detection.

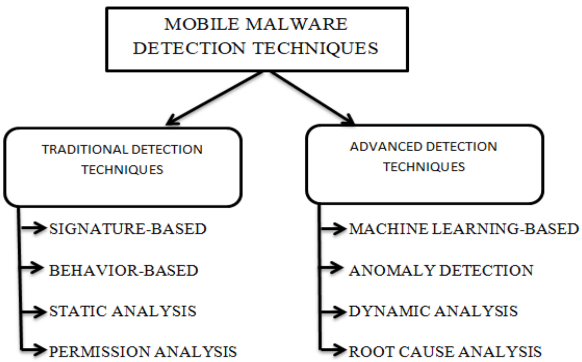

Figure 1. Mobile Malware Detection Techniques

2.1 SIGNATURE-BASED DETECTION

In cyber security, a signature is sometimes referred to as a "pattern" linked to a malicious component that poses a risk to a web server, an operating system (OS), and other computer resources. This pattern could be a byte sequence in network data or a set of bytes inside a file. These patterns can appear as a variety of different things, like criminal behaviors that try to get around security solutions or illegal software execution or network and directory access. Signature-based detection is a traditional mobile malware detection technique that identifies and mitigates the malwares (malicious software) on the mobile devices; this technique creates and compares the digital signatures that are the unique identifiers derived from the traits of known malware [5]. Every file has the proper signatures generated and compared with known signatures that have been previously recognized and stored. The procedure doesn't end until a match is discovered. In this case, the file is automatically stopped since it is deemed dangerous. This detection technique is used by the antivirus products to detect the threats. Additionally, it is well-known for being a crucial component of security systems including firewalls, intrusion detection and prevention systems, address verification services, and intrusion detection systems (IDSs) [6]. The working of signature-based detection is shown in figure 2, the first step is the Signature Generation where the researchers examine the malware samples and extract the unique traits such as behavior patterns, file structures or code snippets Digital signatures are then generated based on these traits. In the next phase the signatures are kept in a centralized signature database, which has a library of signatures representing the known malwares. In the third phase when the user starts a malware scan on the mobile, the antivirus software begins to scan the device’s applications and files and this is the Scanning process in the signature-based technique. In the fourth phase, each application's and file digital signature is carefully compared by the antivirus program with the signatures saved in the database. The next phase detects whether the file or application's signature and the signature in the database match; if they do, the antivirus software detects the file or application as malicious. Depending upon the results of detection phase the antivirus program takes suitable action of deleting the malicious file or application in the next phase. In the last phase the signature database is kept up to date. The researchers continuously detect the new malwares to create signatures for them at last the updates made are distributed among the users by software updates so that the antivirus can detect the latest malicious activities [7].

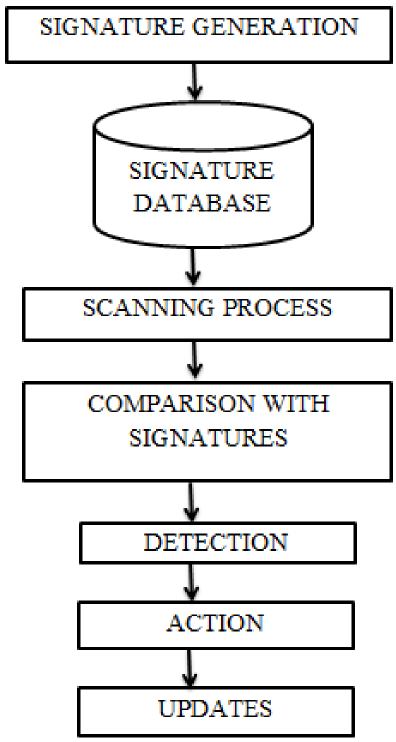

Figure 2. Working of Signature-based Detection

There are various pros and cons of the signature-based mobile malware detection technique. Various advantages of this technique include its effectiveness for identifying and mitigating known malwares, this technique generates the low false positive rate, it is quite low in terms of processing power requirements that is it do not require a lot of RAM or processing power, this technique enables the fast detection and fast response. Few disadvantages of signature-based mobile malware detection techniques are it is ineffective against the zero-day attack; malware is identified only for the signatures that exist in the database, dependency on the regular signature updates is another limitation for this technique [8].

2.2 BEHAVIOR-BASED DETECTION

Behavior-based mobile malware detection technique also aims to identify and mitigate the malwares that target the mobile devices. While the signature-based detection matches known signatures, the behavior-based detection looks for suspicious activity by analyzing software behavior patterns and behaviors. Rather than depending only on predetermined signatures or patterns, this technique seeks to detect harmful actions, such as, suspicious network communication, unauthorized data access and privilege escalation. With this approach, zero-day or previously undisclosed malware can be successfully detected by tracking the actions of programs in real-time [9]. The working of behavior-based mobile malware detection technique includes behavior monitoring, behavior analysis, anomaly detection, dynamic risk assessment, response and mitigation, feedback and learning. In the first step the detection system keeps the track of wide range of activities that includes network connectivity, file access, interactions with confidential data and system calls as they occur within the running programs and processes on the mobile devices. In the second phase, algorithms and heuristics are used to assess the observed actions and find the patterns that indicate the suspicious intent. In this phase the activities are observed and are compared to the observed behaviors against the known behavioral profiles of malware and genuine software. In the third phase anomaly detection techniques are used by the system to find anomalies from the predicted behavior. Any behavior that differs noticeably from the predetermined baseline can be reported as suspicious and subjected to further analysis. In the fourth phase the system gives each process or application a possibility of malicious intent (risk score) based on the anomalies found in the observed behaviors. Depending on how serious a threat is, dynamic risk assessment aids in prioritizing the response. In the next phase the system starts the necessary response measures if it finds that process is having malicious behavior or poses a high risk, this may include terminating its execution, islolating the application, block network communication and many more. In the sixth and the last phase, the detection system improves its effectiveness and accuracy with time from the feedback generated by continuous learning from new data. To improve its behavioral analysis skills and adjust to changing threats, it integrates knowledge from earlier detections [10].

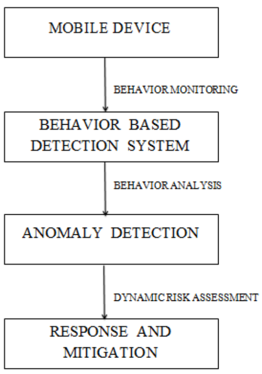

Figure 3. Working of Behavior based detection

Figure 3 explains the working of behavior based mobile malware detection, the mobile device represent the device used for the implementation of the behavior-based malware detection. The core component that is the behavior-based detection system that is responsible to monitor, analyse and respond to the behaviors of processes or applications on the device. Behavior monitoring monitors the behavior in real-time. Behavior analysis identifies the anomalies and patterns of the observed behavior. Anomaly detection detects the abnormalities from the expected or normal behavior. Dynamic risk assessment assigns the risk scores based on the analysis. And response and mitigation initiates correct response measures to mitigate the possible threat.

The advantages of behavior based mobile malware detection technique include detection of zero-day threat, dynamic detection is another advantage of this technique as it focuses on the action of the process or application, this technique continuously learns from the behavior of different applications and can adapt to new types of threats. There are various disadvantages of behavior-based mobile malware detection technique too that include complexity, privacy concern, limited effectiveness against encrypted malware and dependence on behavioral patterns [6].

2.3 MACHINE LEARNING BASED DETECTION

Machine learning (ML) has emerged as an influential tool in the battle against mobile malware. By advanced algorithms and techniques, machine learning-based mobile malware detection systems can analyse large amount of data and automatically identify malicious apps based on patterns and behaviors. Various machine learning algorithms can be utilized for mobile malware detection such as random forests, SVM, decision trees etc. and deep learning models like CNN and RNN. It differs from the traditional detection techniques as ML-based detection proactively identifies and mitigates the emerging threats while traditional techniques depend on the predefined signatures or behaviors to detect the known malwares [11]. Figure 4 describes the working of ML-based detection that involves different steps: in the first step the mobile application data is collected and the data contains both malicious and benign data samples and the machine learning models are trained using these data samples as its basis. In the next step appropriate features are extracted and these features include API calls made, network traffic patterns, code structures, resource usage, permission requested and code structures from the mobile applications in the dataset. This step represents applications in the suitable format for analysis. In the third step model selection is done, various ML algorithms like SVM, decision trees, random forest, CNN, RNN etc. can be employed for mobile malware detection. Factors like nature of dataset, desired accuracy and computational resources decides which algorithm will be used. In the fourth step the ML model is trained on the basis of the features extracted from the dataset. Based on the pattern found in the data, the model is trained to differentiate between the malicious apps and the benign app. To reduce the errors and improve the models prediction capability, this step involves optimization of models parameters. After the model is trained its performance is assessed by using different validation dataset, the evaluation standards including accuracy, F1-score, precision, recall are frequently used. The aim is to ensure that the model minimizes the false positives wile identifying the known and unknown malware samples. The next step is the deployment and real time monitoring, after the evaluation is done successful the model that is trained is deployed for the real-world use this is deployed into mobile devices or integrated into mobile security applications to scan and classify applications in real time. To analyse the incoming apps continuously for malicious behavior and provide alerts to the user or security system on time real-time monitoring allows the model to do all this. In the last and the seventh step continuous update and refinement of ML model is important as mobile malware is continuously increasing. This step involves incorporating feedback from the detected threats, retaining the model with new data, and adapting to growing attack techniques [12].

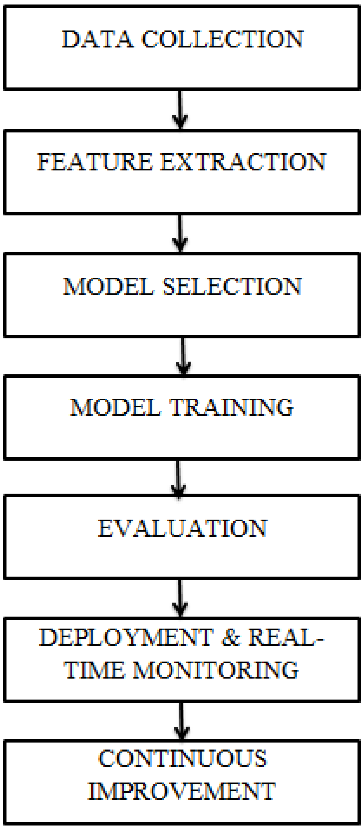

Figure 4. Working of ML based detection

The ML model learns continuously from the new data and can adapt to the growing treats or attacks, this technique handles the large amount of data efficiently and make it suitable for the analyses of large amount of mobile applications, it can proactively identify the developing threat and helps to mitigate the risk before they increase, these are some advantages of ML based detection. Various disadvantages of ML-based detection includes large amount of data requirement for training, overfitting is another issue in this detection, ML models are vulnerable to adversarial attacks, some ML models can be complex and difficult to interpret [13].

2.4 ANOMALY BASED DETECTION

Anomaly based detection is an advanced detection technique that focuses on identifying the malware or detect any unusual pattern or deviations from normal behavior. Anomaly based detection can flag the abnormal activities that indicate the presence of malware as it continuously monitor and analyse the behavior of mobile applications. Anomaly-based detection methods analyze variations from typical system behavior that can point to malicious activities, providing a proactive and dynamic approach to mobile malware detection. Atypical user behavior, unexpected system resource utilization, and strange network traffic patterns are just a few ways in which these anomalies can appear. By focusing on anomalies and deviations from the norm, this technique improves the security position of mobile devices and help to guarantee a safer digital experience for users [14].

The working of anomaly based detection follows various steps that are shown in figure 5, first the baseline is established of normal behavior for various aspects of mobile applications that include battery consumption, network usage, CPU usage etc. a large dataset of legitimate applications derives this baseline. Secondly, the behavior of installed applications is monitored continuously various metrics and activities are tracked in real time that compares them to the established baseline. In the third step anomaly detection is done from the established baseline any deviation is identified as a potential anomaly and the deviation can be in the form of unusual battery drainage, unexpected CPU consumption etc. In the next step appropriate features are extracted from the observed anomalies. Feature extraction includes time of occurrence, the affected system resources, the type of activity and associated metadata. In the fifth step machine learning algorithms are utilized by the anomaly detection techniques to classify the observed anomalies as benign or malicious. In the next step on the observed behavior the system continuously adapts and updates its baseline and ML model as new apps are installed and the existing apps are updated. In the last step when any anomaly is detected the system alerts to notify the user. Depending on how serious the anomaly is and how the system is set up, automated actions like app quarantine, user notification etc. may be started [15].

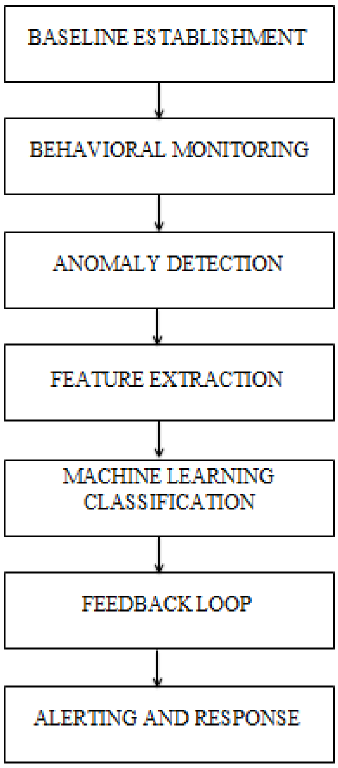

Figure 5. Working of Anomaly based detection

3. Literature work

Alireza Souri and Rahil Hosseini (2018) [16] systematically examines and surveys malware detection strategies that utilize facts mining strategies, with a specific recognition at the dynamic traits of evolving malware. Their research contrasts the strengths and weaknesses of diverse detection methods, emphasizing their effectiveness in classifying malware. By tackling the limitations in malware detection and exploring key methodologies, the paper makes a valuable contribution to the progress of research on this area. The experimental effects display that Support Vector Machine (SVM) is the maximum typically used technique, with a detection rate of 29%, particularly for signature-primarily based malware detection. Other related finding techniques are Bayes Fusion contributes five%, Decision Tree contributes 14%, Naive Bayes contributes 10%, and J-forty eight contributes 17%, with the help of SVM displaying the very best overall performance in instances containing signature-primarily based detection. Ruitao Feng, Sen Chen et al. (2019) [19] discusses the need of conducting Android malware detection immediately on mobile devices, citing safety dangers stemming from unofficial app sources. It underscores the drawbacks of relying on traditional server-aspect detection for programs from unofficial resources, underscoring the importance of getting a very last layer of protection on cellular devices. Their studies examines the effectiveness of various characteristic extraction techniques and categories for deep studying on cell gadgets, along side the precision of various deep neural networks for actual-time detection. It evaluates the effectiveness and dependability of MobiTive, an Android malware detection system preinstalled on six real cellular devices, demonstrating its brief and responsive detection capabilities at once on cell devices. They also addresses the problems of dynamic conduct evaluation-focused malware detection systems in evaluation to static evaluation, underscoring the importance of in addition research in both methodologies. Amira B Sallow et al. (2020) [17] emphasizes on static and dynamic evaluation for cellular malware detection tactics at the maximum famous open systems- Android in recent five years. Researchers investigated diverse gadget gaining knowledge of and deep leaning schemes. A comparison of malware detection the use of apps Call behaviour. It can discover whether or not an app is malicious or benign. For example, SVM stands for the Support Vector Machine. “Call graph extraction and characteristic technology” enclosure is a basis. Call sequencing refers to the sequentially ordered breakdown of a cellular application and its interaction with it. For example Decision Trees can produce a decision tree, whilst Deep learning fashions can be given uncooked name sequences and convey sequences of deep mastering version parameters. Each encasement includes a predetermined technique. Researchers made masses of development in malware detection device. Some of them encompass: Static and dynamic evaluation, Anomaly-based detection, Evolutionary computing to enhance the accuracy of Android malware detection, Creating and education anomaly detection schemes and hybrid scheme packages. Authors additionally created hybrid detection structures, light-weight gadget studying models, and stop-to-give up deep studying structures. Vasileios Kouliaridis et al. (2020) [14] observed that detecting mobile malware has become essential as popular platforms such as Android and iOS face growing vulnerabilities, resulting in a billion-dollar industry that exploits victims for revenue. Research classifies detection methods into static and dynamic approaches, with some viewing them as subsets of signature and anomaly-based techniques. Their survey offers a thorough exploration of mobile malware detection methods from 2011 to 2018. By categorizing and analyzing the detection approaches outlined in various studies, the aim is to shed light on the changing terrain of malware detection and Several studies suggest novel detection systems such as mobile botnet classification using permissions and API calls, malware detection via permission analysis, automated malware detection systems that scan for malicious patterns, and information flow analysis for detecting malware. Dynamic anomaly-based detection enables the identification of unfamiliar malware and zero-day attacks, yet encounters difficulties with false positive rates. Maryam Shahpasand et al. (2020) [18] focuses on the ML models for malware detection, it delves into the utilization of Machine Learning (ML) methods in the realm of security, with a specific focus on malware detection. Adversarial Attack and Defense Techniques: Investigates the adaptation of attack and defense tactics from the image domain to the realm of malware. The review underscores the susceptibility of ML models to Adversarial Examples (AE) in security scenarios, including malware detection. Through a thorough review of existing literature, the paper establishes the groundwork for its exploration of feature-based adversarial attacks on ML classifiers within the realm of mobile malware detection. A critical awareness is on transferring assault techniques from the photograph domain to the malware area, with the aim of advancing the comprehension of hostile assaults and defense strategies within the field of cell malware detection. ÖMER ASLAN and REFIK SAMET (2020) [7] gave a detailed analysis of different malware detection techniques, highlighting the growing threat posed by malwares and need for effective mechanisms aimed at detecting them. Also looks into several detection approaches such as signature-based, heuristic-based, behavior-based, model checking-based, cloud based, deep learning-based, mobile devices-based and IoT based methodologies. Highlighted various research findings and techniques used in identifying malware thereby outlining the strengths and weaknesses of each of these research approaches as well as their methodologies. In addition to that their study points out at the difficulties experienced in distinguishing known and unknown malwares thus emphasizing on need for new methods and approaches that could fill the current gaps in malware detection research. The article touches on limitations and potential improvements related to behavioral based detection strategies, model checking based detection approach as well as cloud based detection technologies. They suggests avenues for further studies to enhance detection accuracy, scalability, evasion resilience against attacks in malware detectors discussing important issues that should be considered when investigating emerging technology trends while addressing present limitations facing this field. Sakil Barbhuiya et al. (2020) [15] focuses on the Smartphone Intrusion Detection Systems (IDSs) are categorized into categories: efficient IDSs and one-magnificence type for phone IDSs. Efficient IDSs encompass signature-based totally and anomaly-based totally systems. Signature-primarily based systems examine application signatures with acknowledged malware signatures, but they may be unable to identify unknown or modified malware. On the opposite hand, anomaly-based totally systems employ system studying algorithms which include SVM, HMM, Naive Bayes, and KNN to song conduct styles. Modern host-primarily based IDSs together with Andromaly, MADAM, and Drebin prioritize light-weight detection on gadgets. Utilizing algorithms like One-Class SVM, one-class classification (OCC) for telephone IDSs includes outlier detection with out requiring a 2d elegance of records. These algorithms are applied for detecting cellphone intrusions, specially specializing in zero-day malware. DroidLight employs one-elegance class (OCC) in dynamic analysis to successfully detect 0-day intrusions on smartphones, even in real-world utilization situations. Researchers have investigated the distribution of malware detection tasks between devices and remote servers to enhance performance. Certain suggested answers encompass preprocessing records on devices and shifting complex device studying duties to servers. DroidLight takes a hybrid method by way of continuously education on a server to increase specific fashions for intrusion detection on devices. Vasileios Kouliaridis and Georgios Kambourakis (2021) [20] summarizes many important works on Android malware detection that have been carried out over the last seven years. It also puts all the studies in the order they were conducted using four determinants; age of dataset, type of analysis, machine learning techniques used and performance metrics. The purpose of this review is to determine what are currently being written about in this field so as to understand how different techniques for detecting Android malware are being developed. It presents a systematic approach, which helps to classify diverse machine learning-based malware detection methods making it easier to choose between them. Moreover, by outlining key elements from each study it assists in identifying similarities and differences between different proposal approaches. They also lays out the ground work for an upcoming discussion about ML based android malware detection methods and unified decision-making model provided in this paper. Rahul Agrawal et al. (2021) [21] explores how the quick-paced increase of the Internet has led to a upward thrust in cyber-attacks and a complicated cybersecurity surroundings. They highlights the importance of employing Deep Learning (DL) and Machine Learning (ML) strategies in community protection to cope with the ever-changing cyber threats. Their research emphasizes the importance of gadget learning systems that target customers and utilize massive facts to become aware of high-danger users and improve employer chance detection. It offers an innovative data engineering method that combines security logs, alert information, and analyst know-how to decorate gadget learning models for cybersecurity. The paper also explores the difficulties encountered in cyber safety operations, underscoring the elaborate nature of turning in cyber security and the significance of Security Information and Event Management (SIEM) systems in identifying malicious behaviors. Together, these aspects highlight the critical importance of cutting-edge technology inclusive of deep gaining knowledge of (DL), gadget learning (ML), and user-targeted gadget getting to know structures in strengthening cybersecurity measures and responding to the ever-evolving cyber danger environment. Cagatay Catal et al. (2021) [22] introduces a Systematic Literature Review (SLR) that facilities on the utilization of Deep Learning (DL) techniques for detecting mobile malware. The evaluation worried the exam of forty journal articles, which have been labeled in keeping with device mastering kinds, DL algorithms, assessment metrics, function selection techniques, datasets, and DL execution platforms for an intensive evaluation. They emphasizes the recognition of Convolutional Neural Networks and Deep Neural Networks within DL algorithms, wherein API calls, Permissions, and System Calls are recognized as the prominent features applied. Supervised getting to know and static features have been the top choices for system studying techniques and statistics sources. Thier study addresses a remarkable hole in existing literature as it is the first Systematic Literature Review (SLR) to thoroughly examine research using Deep Learning for cellular malware detection. It offers treasured views at the usage of Deep Learning algorithms for this urgent difficulty, offering a thorough precis of the modern advancements within the subject. The studies method covered large database searches, snowballing techniques, and strict choice criteria to guarantee the incorporation of topnotch articles. The exclusion criteria have been exactly mentioned, and a collaborative balloting gadget was employed to select primary studies, thereby improving the credibility of the assessment technique. B. Bhaskar et al. (2023) [23] studied Android and iOS cell structures are attractive targets for malware as they manage sensitive records on smartphones, ensuing in a rise in vulnerabilities aimed toward mobile devices. Detecting Android malware is important in the realm of cellular safety, emphasizing current malware attacks, vulnerabilities, detection strategies, and protection remedies. Machine studying techniques have validated potential in enhancing the accuracy of malware detection on Android devices, outperforming other current strategies. Researchers have counseled multiple machine learning algorithms including SVM, NB, or DNN for detecting Android malware, highlighting the significance of incorporating gadget gaining knowledge of into phone security. The model showcased SVM Category Classification accuracy of over ninety three% and ANN Category Classification accuracy of greater than 90. Eighty two%, demonstrating its efficacy in pinpointing malicious programs. The upward push in Android malware has spurred vast studies into detection methods, with a specific emphasis on leveraging device gaining knowledge of-primarily based tactics to efficaciously pick out Android malware. The studies underscores the necessity for effective techniques to analyze and discover Android. Marco Anisetti et al. (2023) [24] noticed that the machine learning and deep studying have gained significance in malware detection, in particular in static evaluation that concentrates on facts extracted from every malware and valid code, inclusive of Windows API calls and Assembly commands. Static assessment techniques, leveraging more than a few classifier algorithms, frequently achieve immoderate tiers of accuracy, precision, and keep in mind exceeding 0.Nine, albeit they may be intrusive. Dynamic evaluation overcomes the regulations of static analysis by way of using addressing encryption, obfuscation, and polymorphism, on the equal time as hybrid evaluation merges static and behavioral facts to enhance detection abilties. Lightweight malware detection, which relies on dynamically studying primary features generally disregarded through the usage of traditional detectors, represents a burgeoning situation displaying encouraging outcomes. The venture of confined information in malware detection may be tackled through artificial facts technology strategies which incorporates Generative Adversarial Networks (GANs) and Variational Autoencoders. Time collection data, mainly while making use of LSTM fashions, has established its effectiveness in classifying malware, supplying a promising approach for detection. Christopher Jun Wen Chew et al. (2024) [25] explores the progress in Android security measures over the years, culminating within the present day security panorama. They outline numerous forms of ransomware, imparting insights into extraordinary classifications of malicious software. Also explores the ancient improvement of malware evaluation techniques, contrasting static and dynamic methods. They emphasizes the challenges of static evaluation in figuring out complex malware and the effectiveness of dynamic analysis against obfuscation techniques. The gadget call obfuscation approach brought by way of Srivastava et al. As a approach to hide malicious activities at some point of dynamic analysis. The assessment concludes by means of underlining how the paper's actual-time machine call-primarily based ransomware detection method can enhance modern-day malware detection techniques. It affords a wonderful approach that doesn't rely on gadget studying models or sandbox environments, placing it aside from systems like DNADroi. Mawj faez Mahdi and Sarah Saadoon Jasim (2024) [26] observed that mobile malware assaults are at the upward thrust, specially targeting the open-source Android platform because of its substantial adoption. Prior studies on mobile malware detection applied diverse metrics, models, and datasets, posing challenges when making comparisons. Three primary classes of methodologies for malware detection are recognized: static evaluation, dynamic analysis, and hybrid evaluation. While static analysis is easier to installation, dynamic analysis can gain comparable or superior consequences in certain situations. Hybrid analysis merges the blessings of each strategies. Utilizing gadget getting to know algorithms is critical for achieving high accuracy in malware detection, with efficient function selection being a essential attention. The SVM classifier is usually employed and validated effective in detecting cell malware, whereas deep mastering techniques which include CNN-LSTM display encouraging consequences. Larger datasets, risk detection systems integrated into app stores, and novel feature choice algorithms are a number of the following research avenues to be pursued.

Table 1. Analysis of previous work

Authors	Dataset	Technique	Outcome	Strength	Limitation
Huabiao Lu et al. (2013) [27]	Mwanalysis.org malware executable were 331 samples clustered into 8 families	Behavioral Signature Generation System, SimBehavior	SimBehavior extracts the behavioral signatures effectively. The	Lightweight behavioral signature generation system for malware	Behavior graph complexity in network security. Difficulty in detecting

			generated signatures are efficient and suitable for malware detection.	detection in PCS. Syscall-based behavior capture for precise program intent identification. Kernel monitor for syscall sequences collection from malware samples.	malware using behavior graph. Handle and ordering dependencies as indicators of program behavior.
Min Zheng et al. (2013) [28]	DroidAnalytics used 150,368 Android applications for analysis. Extracted 47,126 full path methods from Android SDK 4.1 version.	Signature-based analysis, permission recursion technique.	DroidAnalytics detects 2,494 malware samples from 102 families. Detects 342 zero-day malware samples from six different families. Effective in analyzing malware repackaging and mutations.	DroidAnalytics effectively detects 2,494 Android malware samples from 102 families. The system can analyze malware and mutations efficiently.	Signature-based analysis may not be effective against evasion techniques like polymorphism or metamorphism. The evaluation of DroidAnalytics may not fully represent the diversity of Android malware in the wild.
Vinit B. Mohata et al. (2013) [29]	OpenVC dataset used for training and enhancing malware detection models	Malware detection techniques include behavioral analysis and data mining methods.	Malware detection involves analysis, classification, detection, and containment	Malware detection strategies for smartphones with open-source platforms. Analysis of	Limitations focus on mobile phone functionality for malware detection. Proposes limitation-

		Cloud-based detection involves scanning Google Play apps for malware.	of malware. Commercial antivirus uses signature-based techniques for malware detection	malware propagation methods and containment techniques	oriented techniques for effective malware detection and prevention
Khurram Majeed et al. (2014) [30]	Real life data consisting of application usage statistics, contextual information from mobile devices and various system metrics	Behavior-based anomaly detection framework for mobile devices using K-Means clustering.	Behavior-based anomaly detection framework for smartphones with high accuracy. Optimum number of clusters determined for user profiles with good accuracy.	Novel approach with high accuracy in user behavior profiling. Implementation of unsupervised machine learning technique for real-time malicious activity detection.	Limited to signature-based antivirus scanners, unable to detect new malware. Behavior-based anomaly detection tested on mobile devices, not smartphones.
Joshua Abah et al. (2015) [31]	Dataset used for research includes features from application layer. Dataset focuses on monitored features from SMSs, calls, and device status	Anomaly-based detection systems use feature vectors to train the classifier. Machine learning approach with K-NN classifier detects real Android malware.	Detection system achieved 93.75% accuracy with low false positive rate. Classifier performance showed high accuracy and low error rate.	Detection system accuracy: 93.75%, low error rate: 6.25%, low false positives.	Signature-based detection techniques are becoming inefficient in detecting new malware. Limitation in detecting new and unknown malware on Android platforms.
Abdullah J.	SMS Spam	Pattern-	Successfully	MONET	Some SMS

Alzahrani and Ali A. Ghorbani(2015) [32]	Collection, labelled spam and normal SMS. Dataset includes 1,353 spam SMS text messages and unlabelled dataset with 55,835 messages.	matching and rule-based techniques are used for SMS botnet detection. SMS Feature Extractor is implemented to process incoming and outgoing messages	detected all 747 malicious SMS messages with a 100% detection rate and no false negatives. Flagged 351 SMS messages as suspicious.	defends against 10 obfuscation and transformation techniques with 7% performance overhead. It alerts users automatically with intrusion details to prevent malicious behaviors.	messages are labeled as suspicious, requiring user decision-making. Blocking known botnet SMS using rules and patterns is not sufficient to cut the C&C channel.
Andrea Saracino et al. (2016) [33]	Genome dataset: 1,242 malicious Android apps from 49 malware families.	MADAM uses a similarity-based K-NN classifier for malware detection.	MADAM effectively blocks over 96% of malicious apps. It detects and stops malicious behaviors from 125 malware families. MADAM has an accuracy of 96.9% in detecting malware samples.	MADAM has low false alarm rate, negligible performance overhead, and limited battery consumption. MADAM accurately identifies 40 families of SMS Trojans.	Behavior-based detection is vulnerable to poisoning and mimicry attacks. MADAM may signal some apps as dangerous despite unclear classification.
Mingshen Sunet al.(2016) [34]	3,723 malware samples from Android Malware Genome Project, DroidAnalytics, contagio minidump forums. Top 500 apps	MONET uses interception techniques on binder and system calls.	MONET achieves 99% accuracy in detecting malware variants.	MONET defends against 10 obfuscation and transformation techniques	Limited applicability to Android 5.0 Lollipop's ART runtime. Extending MONET to

	from Google Play market for true negative evaluation	Hooking technique injects libraries into apps for interception. MONET intercepts binder calls at JNI interface and Service Manager	Defends against 10 obfuscation and transformation techniques with minimal overhead. Automatically alerts users with intrusion details to prevent malicious behaviors	with 7% performance overhead. It is a comprehensive system that includes backend detection server and client app for mobile devices.	adapt to the ART runtime is necessary for continued effectiveness.
James Scott (2017) [35]	The OpenVC dataset is utilized for training and enhancing models	The research discusses the ineffectiveness of signature-based malware detection. Malware now uses AI for signature alteration, evasion, and obfuscation	Cybersecurity needs predictive, preventative, and protective AI solutions. AI endpoint security can preempt and mitigate known and unknown threats. Organizations must rely on machine learning AI for scalable protection.	Malware includes intelligent deception, obfuscation, and evasion components.	Products rely on signatures for detection when samples are small. Lack of advanced AI protection makes critical infrastructure vulnerable.
Panagiotis I. Radoglou-Grammatikis, Panagiotis G.	CTU-13 dataset used for training with 145438 NetFlows.	Anomaly detection technique using artificial	Proposed IDS detects Android system anomalies	Lightweight IDS with MLP neural network detects	High false alarm rate and gigabit speeds scaling. Existing

Sarigiannidis (2017) [36]		neural network for Android mobile devices. Feature extraction module to detect abnormal behaviors in network traffic	with 85% accuracy. Detection rate of the system reaches 81%. Future work aims to enhance accuracy and detection rate further.	Android mobile anomalies effectively. ANN efficiently processes NetFlow data for intrusion detection.	methods are derived from PC anomaly detection techniques.
Zhenxiang Chen et al. (2018) [37]	5560 malware samples from Drebin Project used for dataset creation. Top 24 malware families with active distribution included in the dataset.	Synthetic minority oversampling technique (SMOTE) for imbalanced classification. Support vector machine (SVM) cost-sensitive method for imbalanced data. C4.5 cost-sensitive method used for imbalanced classification	IDGC model shows stability with AUC and GM between 0.8-1.0. S-IDGC model improves efficiency by reducing time consumption significantly.	IDGC model strengthens minority class and weakens majority class samples. Prototype system allows users to compare classification algorithms effectively.	Common imbalanced classification algorithms degrade significantly at certain imbalance rates. Performance degradation occurs when imbalance rate threshold is reached.
Shanshan Wang et al. (2018)	Malicious apps from Drebin project, 5560 real malware samples. Normal apps downloaded from popular app markets, 8321 samples	Classify malware based on similarities in URLs extracted from HTTP	Proposed method achieves 97.89% detection rate for Android	Lightweight framework for Android malware identification with high detection	Limited by the availability of existing malicious samples for training, which affects the wide

		requests. Generate state signatures by observing traffic over a long period. Identify CC channels within malware traffic to counter obfuscation techniques	malware.	accuracy. Combines network traffic analysis with machine learning algorithm for effective detection. Achieves a detection rate of 97.89% when combining two detection mechanisms	applicability of the method. The number of malware families and samples is crucial for the effectiveness of the approach.
Ruitao Feng et al. (2019)	Dataset includes 21,499 benign and malicious samples for experiments. Sources of dataset: Drebin, Genome, Contagio, Pwnzen, VirusShare.	Deep learning-based approach for Android malware detection. Testing techniques for deep neural networks to evaluate model quality.	MobiDroid provides reliable detection accuracy of over 97%. Detection service on mobile devices is reactive in less than 10 seconds.	Deep learning-based Android malware detection system with real-time response. Migration of DL model to TensorFlow-lite for mobile platform efficiency. Combined feature model outperformed single feature models in malware detection.	Limited application dataset affects deep learning-based malware detection. Hardware performance of Android devices can impact detection time.
Amira B. Sallow et al.(2020) [17]	An Android dataset with benign and malicious apps for analysis. Dataset used for behavioral pattern analysis in Android	Static and dynamic analyses used for feature derivation	Proposed system achieved high accuracy in malware	Android platform vulnerabilities and malware detection strategies	The paper lacks discussion on real-world implementation challenges.

	malware detection	and selection. Principle Component Analysis (PCA) applied to reduce feature dimensions. Support Vector Machine (SVM) utilized for malware classification.	detection. Detection techniques based on machine learning and hybrid systems.	discussed comprehensively. Android designed as open-source with high-level technologies for user data. Proposed Android malware hybrid detection scheme for high efficiency.	
Cagatay Catal et al. (2021) [22]	Drebin and VirusShare, Android Malware Genome Project, AMD dataset, and more.	Feature selection techniques include Random Forest, InfoGain, SAILS, Relief, Boruta	Framework for benchmarking deep learning-based approaches and experimental design enhancement. Focus on multi-modal and semi-supervised deep learning techniques for malware detection.	Convolutional Neural Networks and Deep Neural Networks are widely used. API calls, Permissions, and System Calls are dominant features.	Challenges include dataset availability, model building steps, and network traffic features
Rahul Aggarwal et al. (2021) [21]	The OpenVC dataset is utilized to train and enhance models	Signature-based scan technique.	Description of static and dynamic malware analysis	Android malware analysis methods include static	Database update, permission, background run, battery

			methods and automation guidelines. Utilization of algorithms for malware classification and hooking software techniques.	and dynamic techniques. Malware detection algorithms and signature analysis using hooking software are utilized. Focus on lower-level microarchitecture features for malware exploit detection.	consumption are limitations.
Ahmed S. Shatnawi et al. (2022) [38]	CIC InvesAndMal2019	Static base classification approach for Android malware detection based on android permissions and API calls	SVM, KNN, NB are used for classification SVM classifier achieved the highest accuracy rates with an average of 94% accuracy using permission features and 83% accuracy using API call features.	Utilizes comprehensive new Android malware dataset Employs well-known Machine Learning algorithms for classification Achieves high accuracy rates in malware detection.	Static base classification approach may not capture dynamic behaviors of malware Relies on permissions and API calls. Limited to the specific dataset used (CIC InvesAndMal2019)
Sriyanto et al. (2022) [39]	Dataset used for research was abnormal and required normalization methods. Data was collected in the form of log data from	Min-Max normalization and logarithm function for accuracy, Ten Fold	MiMaLo achieved 93.54% accuracy and 0.982 AUC using neural	MiMaLo method increased classifier performance, especially Neural	Feature selection methods did not produce high-performance models. Static analysis can be

	Android systems.	Cross Validation technique, Hybrid analysis	network	Network. Support Vector Machine had the highest recall and precision values.	avoided through obfuscation or encryption techniques. Sensitive data flow gains are less complex to analyze. Dynamic Analyst approach requires high computational power and storage space.
B. Bhaskar et al.(2023) [23]	Dataset consists of safe and harmful apps for Android malware detection	Android malware detection technique involves neural network model. Scikit-learn provides tools for identifying hate speech. Pickle module in Python is used for serializing and de-serializing objects.	Proposed model shows accuracy comparable to existing models with less resources. Android malware poses a significant threat to user data and device security. Model aims to provide online service for malware assessment before download.	Improved precision and dependability in Android malware detection. Utilizes a neural network model trained with safe and harmful apps. Critical examination of existing mobile malware frameworks for reliable detection.	Cumbersome interface design with minimal features for classification
Marco Anisetti et al.(2023)	Real-world malware from VirusShare, 5,000 PE Windows	Behavioral-based malware	Achieved 0.99 accuracy	Lightweight malware detection	

[24]	files.	detection, Utilized LSTM network trained on augmented datasets for malware detection	using LSTM network for malware behavioral patterns.	approach based on system performance data. Combines deep learning with easily accessible behavioral data for detection. Hybrid analysis improves detection by combining static and behavioral information.	
Mawj faez Mahdi and Sarah Saadoon Jasim(2024) [26]	MH-100K, CICAndMal2017, CICInvesAndMal 2019, CCCS-CIC-AndMal-2020, Andro-AutoPsy.	The research paper focuses on mobile-based malware detection using AI techniques. The SVM classifier is widely used in machine learning for malware detection.	Categorizing methods into dataset types, detection methods, and performance evaluation Analysis of techniques from feature-based and classifier perspectives. SVM classifier functions effectively with clear margins and fewer	Utilizes artificial intelligence for mobile malware detection with diverse datasets. Classifiers like SVM and CNN-LSTM yield favorable outcomes in malware detection. Focuses on static, dynamic, and hybrid analysis for malware detection	Large datasets with noise reduce system performance. High computational cost and time consumption

			samples. Future research focus on feature selection and dynamic analysis for malware detection		
Christopher Jun Wen Chew et al. (2024) [25]	Dataset available upon request through vimal.kumarwaikato.ac.nz.	Real-time system call-based ransomware detection technique, Methodology involves extracting system call logs and identifying common patterns	Identified 12 common high-level behavioural patterns in system calls. Detected malicious patterns and false positives in ransomware detection evaluation.	Utilizes regular expressions and finite state machines for real-time detection. Focuses on high-level system call behavioural patterns exhibited by ransomware.	Detection system unable to identify fine-grain details due to abstraction. Proposed streaming approach has known limitations in detecting crypto ransomware

4. Conclusion

The hazard landscape of malware continues to conform, posing significant challenges to customers, corporations, and cybersecurity specialists. examined the many malware detection methods, encompassing both conventional and advanced approaches, in order to identify their advantages, limitations, and uses. Signature-based detection stays a cornerstone of malware detection, offering effectiveness in figuring out regarded threats but falling quick towards 0-day assaults. Behavior-based detection offers a proactive method via studying software conduct styles but may also battle with fake positives and encrypted malware. Machine mastering-based detection leverages superior algorithms to analyze big datasets and pick out emerging threats, while anomaly-primarily based detection specializes in deviations from ordinary behavior to locate unknown malware. The literature assessment has highlighted the importance of adopting a multi-faceted method to mobile malware detection, integrating unique techniques to decorate detection accuracy and resilience towards evolving threats. Future studies ought to attention on overcoming the constraints of modern-day detection methods, consisting of improving the accuracy of anomaly-primarily based detection and addressing the challenges of adversarial assaults on machine mastering models. Overall, this contributes to the body of knowledge in cybersecurity by means of supplying insights into mobile malware detection techniques and proposing avenues for destiny studies to bolster the security posture of cellular devices and protect users' privacy and statistics.

REFERENCES

1. Caviglione, L., Choraś, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M. and Wasielewska, K., 2020. Tight arms race: Overview of current malware threats and trends in their detection. *IEEE Access*, *9*, pp.5371-5396.
2. Zimba, A., Wang, Z., Chen, H. and Mulenga, M., 2019. Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. *KSII Transactions on Internet and Information Systems (TIIS)*, *13*(6), pp.3258-3279.
3. Sadeghpour, S. and Vlajic, N., 2021. Click fraud in digital advertising: A comprehensive survey. *Computers*, *10*(12), p.164.
4. Sadeghpour, S. and Vlajic, N., 2021. Click fraud in digital advertising: A comprehensive survey. *Computers*, *10*(12), p.164.
5. Venugopal, D. and Hu, G., 2008. Efficient signature based malware detection on mobile devices. *Mobile Information Systems*, *4*(1), pp.33-49.
6. Chakravarty, A.K., Raj, A., Paul, S. and Apoorva, S., 2019. A study of signature-based and behaviour-based malware detection approaches. *Int. J. Adv. Res. Ideas Innov. Technol*, *5*(3), pp.1509-1511.
7. Aslan, Ö.A. and Samet, R., 2020. A comprehensive review on malware detection approaches. *IEEE access*, *8*, pp.6249-6271.
8. Malhotra, A. and Bajaj, K., 2016. A survey on various malware detection techniques on mobile platform. *Int J Comput Appl*, *139*(5), pp.15-20.
9. Vanjire, S. and Lakshmi, M., 2021, September. Behavior-based malware detection system approach for mobile security using machine learning. In *2021 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-4). IEEE.
10. Dai, S., Liu, Y., Wang, T., Wei, T. and Zou, W., 2010, September. Behavior-based malware detection on mobile phone. In *2010 6th international conference on wireless communications networking and mobile computing (WiCOM)* (pp. 1-4). IEEE.
11. Liu, K., Xu, S., Xu, G., Zhang, M., Sun, D. and Liu, H., 2020. A review of android malware detection approaches based on machine learning. *IEEE access*, *8*, pp.124579-124607.
12. Herron, N., Glisson, W.B., McDonald, J.T. and Benton, R.K., 2021, January. Machine learning-based android malware detection using manifest permissions. Proceedings of the 54th Hawaii International Conference on System Sciences.
13. Senanayake, J., Kalutarage, H. and Al-Kadri, M.O., 2021. Android mobile malware detection using machine learning: A systematic review. *Electronics*, *10*(13), p.1606.
14. Kouliaridis, V., Barmpatsalou, K., Kambourakis, G. and Chen, S., 2020. A survey on mobile malware detection techniques. *IEICE Transactions on Information and Systems*, *103*(2), pp.204-211.
15. Barbhuiya, S., Kilpatrick, P. and Nikolopoulos, D.S., 2020, January. DroidLight: Lightweight anomaly-based intrusion detection system for smartphone devices. In *Proceedings of the 21st international conference on distributed computing and networking* (pp. 1-10).
16. Souri, A. and Hosseini, R., 2018. A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-centric Computing and Information Sciences*, *8*(1), pp.1-22.

17. Sallow, A.B., Sadeeq, M., Zebari, R.R., Abdulrazzaq, M.B., Mahmood, M.R., Shukur, H.M. and Haji, L.M., 2020. An investigation for mobile malware behavioral and detection techniques based on android platform. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *22*(4), pp.14-20.
18. Shahpasand, M., Hamey, L., Kaafar, M.A. and Vatsalan, D., 2020, November. Feature-Based Adversarial Attacks Against Machine Learnt Mobile Malware Detectors. In *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-8). IEEE.
19. Feng, R., Chen, S., Xie, X., Ma, L., Meng, G., Liu, Y. and Lin, S.W., 2019, November. Mobidroid: A performance-sensitive malware detection system on mobile platform. In *2019 24th International Conference on Engineering of Complex Computer Systems (ICECCS)* (pp. 61-70). IEEE..
20. Kouliaridis, V. and Kambourakis, G., 2021. A comprehensive survey on machine learning techniques for android malware detection. *Information*, *12*(5), p.185.
21. Agrawal, R., Sharma, Y., Awasthi, H. and Landge, P., 2021. A signature-based malware detection system. *International Journal of Recent Advances in Multidisciplinary Topics*, *2*, pp.115-118.
22. Catal, C., Giray, G. and Tekinerdogan, B., 2022. Applications of deep learning for mobile malware detection: A systematic literature review. *Neural Computing and Applications*, *34*(2), pp.1007-1032.
23. Bhaskar, B., Sharanya, S., Murali, A.B., Archana, E. and Mohanaprakash, T.A., 2024. Protectors of the Android Domain: Research into Mobile Malware Detection and Defense. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(1), pp.639-646.
24. Anisetti, M., Ardagna, C.A., Bena, N., Giandomenico, V. and Gianini, G., 2023, May. Lightweight behavior-based malware detection. In *International Conference on Management of Digital* (pp. 237-250). Cham: Springer Nature Switzerland.
25. Chew, C.J.W., Kumar, V., Patros, P. and Malik, R., 2024. Real-time system call-based ransomware detection. *International Journal of Information Security*, pp.1-20.
26. Jasim, S.S., 2024. Mobile based Malware Detection using Artificial Intelligence Techniques a review. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, *16*(1), pp.105-116.
27. Lu, H., Zhao, B., Su, J. and Xie, P., 2014. Generating lightweight behavioral signature for malware detection in people-centric sensing. *Wireless personal communications*, *75*, pp.1591-1609.
28. Zheng, M., Sun, M. and Lui, J.C., 2013, July. Droid analytics: a signature based analytic system to collect, extract, analyze and associate android malware. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 163-171). IEEE.
29. Mohata, V.B., Dakhane, D.M. and Pardhi, R.L., 2013. Mobile malware detection techniques. *Int J Comput Sci Eng Technol (IJCSET)*, *4*(04), pp.2229-3345.
30. Majeed, K., Jing, Y., Novakovic, D. and Ouazzane, K., 2014, October. Behaviour based anomaly detection for smartphones using machine learning algorithm. In *Proceedings of the International conference on Computer Science and Information Systems (ICSIS'2014), Dubai, UAE* (pp. 17-18).
31. Abah, J. and O V, W., 2015. A machine learning approach to anomaly-based detection on Android platforms. *arXiv preprint arXiv:1512.04122*.
32. Alzahrani, A.J. and Ghorbani, A.A., 2015, July. Real-time signature-based detection approach for sms botnet. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)* (pp. 157-164). IEEE.
33. Saracino, A., Sgandurra, D., Dini, G. and Martinelli, F., 2016. Madam: Effective and efficient behavior-based android malware detection and prevention. *IEEE Transactions on Dependable and Secure Computing*, *15*(1), pp.83-97.

34. Sun, M., Li, X., Lui, J.C., Ma, R.T. and Liang, Z., 2016. Monet: a user-oriented behavior-based malware variants detection system for android. *IEEE Transactions on Information Forensics and Security*, *12*(5), pp.1103-1112.
35. Scott, J., 2017. Signature based malware detection is dead. *Institute for Critical Infrastructure Technology*.
36. Radoglou-Grammatikis, P.I. and Sarigiannidis, P.G., 2017, May. Flow anomaly based intrusion detection system for Android mobile devices. In *2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST)* (pp. 1-4). IEEE.
37. Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L. and Yang, B., 2018. Machine learning based mobile malware detection using highly imbalanced network traffic. *Information Sciences*, *433*, pp.346-364.
38. Shatnawi, A.S., Yassen, Q. and Yateem, A., 2022. An android malware detection approach based on static feature analysis using machine learning algorithms. *Procedia Computer Science*, *201*, pp.653-658.
39. Sahrin, S.B., Faizal, A.M., Suryana, N. and Suhendra, A., 2022. MiMaLo: Advanced Normalization Method for Mobile Malware Detection. *International Journal of Modern Education and Computer Science*, *14*(5), pp.24-33.s