Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319 - 2526

Volume 15 Issue 01s, 2026

A Literature Review on Spy Software Applications

[1]Miss. Sakshi R. Thakre, [2]Dr. Shobha K. Bawiskar

[1]PG Student, Department of Digital & Cyber Forensics, Government Institute of forensic Science, Chhatrapati Sambhajinagar, India.

[2]Assistant Professor, Department of Digital & Cyber Forensics, Government Institute of forensic Science, Chhatrapati Sambhajinagar, India.

Email: [1]sakshithakre006@gmail.com, [2]shobha.bawiskar@gmail.com

Peer Review Information

Submission: 08 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

Forensic Framework, Spyware e-devices, spy applications, Legal ethics, E-surveillance, cybercrimes.

Abstract

This paper presents the analysis of the literature review on the spyware tools which are invading privacy concerns and challenging the forensic investigation procedures. These tools are increasingly used in the illegal activities and due to the lack of standardized methodology it leads to the loss of data, violation of data privacy, inappropriate results and challenging courtroom procedures. This research focuses on the study of spyware tools including software and applications that are used for the covert surveillance. This paper provides the comprehensive review of the existing techniques summarizing their positive and negative outcomes. The literature review studied that there is lot of development in the detection, manufacturing and technical analysis of the spyware tools. It provides the future point of research by the detailed analysis of the existing techniques and methodology. The purpose of this research is to provide the broader view of development in this domain and highlighting the legal and ethical considerations.

Introduction

A spyware software program used to secretly monitor, track, or record a person's activities and data without their knowledge or consent. These devices have become a dangerous tool for stalkers, abusive partners, and corporate spies. When this type of evidence is found on the crime scene it is difficult to extract the evidence from it as it tries to destroy or try to vanish the evidence. Spyware tools are categorized into three main parts-A) Audio B) Video C) GPS Trackers. This research provides the study about existing techniques for analysing these types of evidences and providing scope to develop the framework to forensically analyse these evidences and can be called as admissible in the court of law. And also provides path to analyse these types of evidences to investigators to follow.

Purpose of Topic

1. Privacy Concerns: The spy tools record the sensitive information with the help of camera, audio recorder and GPS tracker and this leads to the privacy violation of individual.
2. Legal forensic methodology: Providing a forensic methodology leads to the ease in the criminal investigation and provides proper SOP to the investigation to follow for investigating these tools.
3. Admissibility of spy evidences in court: Proper SOP leads to the accurate and true results of the investigation which helps to extract the data from tools which is admissible in the court of law
4. Easy surveillance: Accessibility of spyware tools to the normal people leads to the increase in the number of crimes

5. Prevention of spy evidences: Proper forensic SOP is essential because the experts may lose data from the tools by examining it without the proper methodology.

Aim

Examining the existing techniques related to software and application type of spy tools.

Objective

1. To do literature survey on spy software applications and identify research gap.
2. To study impact of the legal and ethical considerations by use of spyware tools.

Literature Review

Selected Samples For Literature Review Criteria (Inclusive And Exclusive) Are:

Inclusive criteria→ Included last 5 years research articles are considered for study purpose.

Exclusive criteria→ Use of AI and machine learning.

Selected Criteria For Spy Software Applications/Tools:

Inclusive→1.Android devices 2. Focused on spy apps and software

Exclusive→ 1. iOS devices

Table 1.

Apps Used	Technique Used	Result	Positive Outcomes	Negative Outcomes
14 spy apps (Assessing the Functionality and Insecurity of Consumer Android Spyware Apps) [1]	1.Reverse enginerring (uses tool like APKtool and JADX to manually analyze test which convert the binary data into human readable format) 2.In-situ testing 3.Network traffic ananlysis 4.Vulnerability testing	4 spyware apps are vulnerable to the data loss over the network. 6 data store their data in URLs without authorized access 1 app have poor security that leads to stealing of victim's data 4 apps failed to delete data after the logging out and deleting the account and can tranfer data without internet using commands	1.provides the spyware apps capabilities 2.provide practical proof 3.Give info about the negligence of the spyware apps vendors	1.Data loss 2.Privacy concerns 3.poor security 4.Transmission of sensitive information
(Notifylos) Android.Spy. 277.origin malware family [2]	Static analysis Network analysis Dynamic analysis Analysis of Google play store protection	The information is transferred from victim's device to the unauthorized location and google play protect service detect the app and failed installation	1.Provide the security feature of Google play protect 2.Develop a forensic methodology 3.provide Security proposal to the other apps from being compromised	1.Vulnerable to the spyware in the initial period. 2.bypass the permission 3.confusion in the analysis of spy apps due to unrevealing of malicious code
mSpy,SpyX, Hoverwatch ,MobileTracker, freeiKeyMonitor, Cerberus, FlexiSPY, Cerberus app, FlexiSPY [3]	In-situ testing Testing by forensic tools (Spyguard and MVT) Testing of apps after uninstallation	In insitu testing Android mobile phones have access to the more information accessible than the ios.In case of Forensic tool testing Spyguard detect only 2 apps and MVT detects 4 apps in android but no info gets from Ios. After uninstallation android remains traces but ios don't.	1.Tool Efficiency 2.Security of Ios 3.Device data is more effective from monitoring network traffic	1.security issues for Android users 2.Limitation of gathering data from Ios 3.Limitation of tools

Anyone spying android camera (Preventive paper) [4]	AAPS app act as defensive and offensive	In case of defensive these app send alerts ad notification to owner and if the phone is lost and owner send the command to aaps app the camera gets active and send the location of device	1.Successful practically in both features. 2.Works as detection and prevention	1.False positive results 2.Anti-theft feature is spyware
83 apps and 323 websites [15]	Static analysis Dynamic analysis (Vulnerability analysis)	29 apps and 65% websites are vulnerable to the stealing of data	1.give guidance about spy websites Found vulnerabilities for prevention	Double victimized Advancement in the spy app
Detection of spy app [6]	ASAINT app for detection	High accuracy of detection (F1 score-0.85) Fast detection90.01sec) Compatible with android spyware	Powerful took Detect network traffic from spy apps	Limited to known spyware Not compatible with ios
.apk file [7]	Monitoring and alerting by collecting logs	Admin app successfully gives info related to call logs,SMS, location	1.Security 2.Can find lost device 3.Loaction 4.Parental monitoring	Privacy violation Risk Legal issues
mSPY UMobix MobileSPY FlexiSPY TheWiSPY [8]	Network traffic analysis using machine learning	The average accuracy was 79% for the binary-class classification and 77% for the multi-class classification. In the multi-class approach, detection accuracy for spyware systems (UMobix, TheWiSPY, MobileSPY, FlexiSPY, and mSPY) was 90%, 83.7%, 69.3%, 69.2%, and 73.4, respectively, and in the binary-class classification, detection accuracy for spyware systems (UMobix, TheWiSPY, MobileSPY, FlexiSPY, and mSPY) was 93.9%, 85.63%, 71%, 72.3%, and 75.96%; respectively.	Validated detection techniques Standard method	Imperfect accuracy Only focused Android OS
Malicious app detection [9]	Machine learning Algorithms	This method provides 93.6% accuracy to detect the malicious application. This paper considered only 22 out of 135 permissions, so the runtime performance also improved by 85.6%.	1.Can detect unknown malware 2.Has accuracy with 93.6%	1.Only limited to the Android detection 2.Traditional apps are not able to detect unknown malware apps.
FlexiSpy, mSpy, HelloSpy [10]	1.Use a query snowballing approach to find a large set	A vast and easily accessible apps on the play store facilitates the intimate partner violence and the existing anti	1.Large scale study of IPS ecosystem. 2.Developed method to successfully	1.The findings shows that it is depressed for victims as these are easily accessible.

	of useful queries 2. Searching for IPS-relevant apps in Google Play 3. Pruning false positives 4.Anti-spyware evaluation	spyware tools are failed to detect such dual use capabilities apps.	identify and classifying these types of apps.	2 Existing anti spyware tool are ineffective.
Spyware application injects in fake puzzle game.[11]	Spyware application development using java.	It is successfully demonstrated that the fully functional spy application can made with access permission can lead to the violation of privacy rights of an individual.	1.Successfully demonstrated how spyware application can be created. 2.Identified Android information.	1.Shows that developers can create malicious application. 2.Give permission for effective access.
mSpy [12]	Experimental and Comparative Analysis	mSpy is an effective tool for real time monitoring and can make traditional forensic tools inefficient to gather information from social media and tracking while forensic tools is able to recover deleted data and mSpy has the ability to monitor in real time without altering the device.	1.Effective tool for real time monitoring for legal use. 2. Can outperform forensic tools and does not require rooting.	1.Highlights that powerful forensic tools fail to extract information from these apps. 2.Interrupts data collection.
Chameleon [13]	Two step approach: 1.Spyware creation. 2.Spyware detection.	The study created behavior -based detection method DroidSmartFuzzer which is effective for network analysis for the spyware created to test based on their identical malicious behavior.	1.Created effective detection method based on fuzz testing. 2.It is able to detect spyware tool that can miss by signature-based behavior.	Android broadcast receiver system is a major vulnerability that creates a "haven" for spyware to intercept sensitive events like calls and texts.
Roving spy bug in legitimate looking app .[14]	Attack and Defense Demonstration	Mobile device can become covert with malware that have the access without internet connection and diificult to analyse with traditional forensic tools. Signature and permission-based scanners are failed to detect as signature is unknown.	1.Developed an anomaly-based technique to detect malware by behavioral pattern.	1.Spyware are effective and can operate without internet connection. 2.Security risk

Scope of Research

The scope of this research is to provide a detailed literature review on the spyware software applications. It focuses on all the spyware tools which invading the privacy concerns and used for the covert surveillance. The aim is to study the tools used, techniques used for the analysis of these types of tools and understanding the positive and negative outcomes based on their results which leads to examine the existing the techniques. It also mentioned the ethical and legal challenges rising due to the nature of spyware tools. As shown in table 1

Critical Analysis

In the digital age of modern technology, the use of spyware is increasing for the surveillance. These devices are used for the legitimate as well as for illegitimate purpose. It is broadly had role in parental monitoring, stalking partner, illegal activities and in government department. The nature of these types of tools is vulnerable for legal and ethical considerations. This are violating the privacy concerns, abusing partner and may also lead to violence.

This paper presents the literature review based on spyware including software and applications which is a means for covert surveillance. This research provides a detailed advancement in the field of covert devices for their detection, analysis and extraction.

In terms of **spy applications**, the review analyzed that these types of applications are creating the threat to the user's privacy of data and the permissions in their smartphones. These apps stealing the information and have an unauthorised access to the user's camera, microphones and their activities. This apps are providing the unauthorised permissions to the device which may be harmful for an individual rights. These types of apps are mainly used in the stalking of partner activities and the parental monitoring for their children's behaviour. This includes apps like mSpy, Cerberus and the researchers develop the detection apps which are used to detect the presence of app in the smartphones and any other unusual activities conflicting with it. Some researchers are focused on the preventive actions in case if the device is lost these apps are able to click the pictures and provide the information about the location. This also includes the technical analysis which provides the proper procedure to deal with these apps involves static analysis, dynamic analysis, network traffic analysis and reverse engineering techniques and whether the apps leave any traces after installation and ensured the effective results. Majorly focused on the android devices rather than iOS due to open and vast usability of Android devices. The limitations in the detection of the iOS devices is due to its strong security concerns. Some research also focused on the review of the vulnerabilities; challenges and the detection techniques used for the spy applications.

While in case of **spy software the research emphasised** that these softwares are monitoring the mobile devices by encoding the malicious code, cryptography and by transferring the apk files which contains certain malwares that are affecting the devices and may lead to the unusual actions which can monitor the smartphone's camera, microphones. This leads to the destruction of privacy rights of an individual. The researchers focused on the categorization of the mobile spyware. Also, the detection techniques are developed using the machine learning monitoring the unusual traffic. These apps are only detecting the the known spyware software and lack to detect the unknown one and majorly focused on the android spy software. Some focused on the effects of the spyware on the mobile devices.

The literature review provides scope that ss this trend is increasing day by day in the crime it is crucial to develop the standard methodology for the forensic analysis of the spyware as it violating the ethical and legal guidelines of an individual and can be admissible as a source of primary evidence.

Ethical Challenges

1. Privacy violations: The nature of spyware tools leads to the invasion of the person's privacy by controlling their own comfort.
2. Psychological Impact: By monitoring someone may also have affect in their relationships and their mental stability.
3. Misleading of information: The information collected from the spy tools can also vulnerable to the misuse and abuse of an individual.
4. Physical impact: The person being spied with uninformed manner can lead to the suicide and can dehumanize.
5. Consent: The uninformed consent of an individual can create a legal conflict.

Legal Challenges

The nature of the spyware devices led to the invasion of the various laws in India as follows:

1. Article 21 of Indian Constitution:

Art 21 of Indian Constitution states about the 'Right to life and Personal liberty' an also includes 'Right to Privacy'. The spyware devices which engage in surveillance should follow the procedure of law with regards to privacy is legitimate. If it fails to do so then it violates the fundamental right of an individual.[15]

2. Section 66(E) of IT Act:

It states about the violation of privacy by capturing, publishing, or transmitting of images of private area of a person without their consent. The spyware devices used for capturing the individual movement or actions without their knowledge or consent in a private setting it leads to the breaching of this section. It includes the penalty up to 3 years imprisonment and fine up to 2 lakhs rupees or both.[16]

3. DPDP Act 2023:

Digital Data Personal Protection Act,2023 involves the laws to protect the individual's digital personal data while allowing for lawful data processing. It requires following;

a) Consent of an individual with exception for lawful purposes such as state functions, medical emergencies and employment.
b) Data fiduciaries have obligations to ensue data privacy, provide data protection and delete data when its no longer needed. The spyware devices evading the individual's privacy and not satisfying the DPDP Act requirements led to the penalty up to 250 crores but exemptions for national security and public order.[17]

Discussion and Future Work

All findings of the literature review discuss that the spyware devices are not only limited to the intelligence and government department but due to the easy availability on the commercial platforms it is accessible to the common people. This stealthy and user-friendly interface of this type of tools leads to the violation of privacy concerns, parental monitoring, stalking partner and challenging investigations.

In case of the **spy applications**, it is inferred that the researchers are focused on the detection of the spy devices in the smartphones. They majorly focus on the Android devices because of its open nature and its vast usability. Also discussed about the vulnerabilities of the android devices for their security reasons and the detections apps also vulnerable to the loss of data. The iOS devices are limitations to this app due to its strong security reasons. It also shows the development of technical analysis for these spy apps. The future work should focus on the detection of spy apps in iOS devices using machine learning and should design the framework for the forensic analysis which can be admissible in the court of law.

Moreover, in case of **spy software**, which is vulnerable to the unauthorised stealing of personally identifiable information using malicious code or any apk files. This spy software is also decreasing the performance of the Android smartphones. By taking these problems in account researchers develop a monitoring system to prevent the loss of information also developed the detection system using machine learning but they lack to develop the standardized procedures for their analysis.

Study showed lack of standard framework which is the major research gap for developing the Standard Operating Procedures (SOPs) for the analysis of these types of spy tools for the purpose of the legal investigation which is admissible in the court of law as evidence with ethical considerations

Research Gap

1. Detection of Hardware spy devices.
2. Analysis of hardware spy devices.
3. Standard procedure for analysis of spy tools.
4. Only focuses on COTS spyware tools.

Conclusion

The increasing use of the spyware tools in the crimes leads to the breaching of privacy concerns, legal and ethical considerations. This paper studied that the researchers developed many detection and preventive techniques for the spyware including software and applications to avoid the violation of sensitive information with uninformed consent. Some focused on the manufacturing and technical analysis which shows the high accuracy results. In the technical analysis, they provide a step-by-step guidance to examine the spy tools. Many apps were developed for the detection of spy tools which provide valuable information. Here vulnerabilities, challenges, positive and negative outcomes are also highlighted. And the researchers are trying to solve this problem. This paper presents the detailed analysis of the spyware tools which provides the scope to carry forward the research in this domain.

References

[1] Liu, E., Rao, S., Havron, S., Ho, G., Savage, S., Voelker, G. M., & McCoy, D. (2023). No privacy among spies: Assessing the functionality and insecurity of consumer android spyware apps. *Proceedings on Privacy Enhancing Technologies*.

[2] Hutchinson, S., & Karabiyik, U. (2019). Forensic analysis of spy applications in android devices.

[3] Caruso, A. (2024). *Forensic Analysis of Mobile Spyware: Investigating Security, Vulnerabilities, and Detection Challenges in Android and iOS Platforms* (Doctoral dissertation, Politecnico di Torino).

[4] Wanjale, V., Dhapte, A., Morey, S., & Koria, M. N. (2014). AAPS Android Based System for Camera Based Attacks. *International Journal of Emerging Technologies and Engineering (IJETE)*, *1*(10), 2348-8050.

[5] Mannan, M., Youssef, A., Mangeard, P., Yu, X., Tejaswi, B., & Pagey, R. (2023). *Privacy analysis of technologies used in intimate partner abuse*. Technical Report. Concordia

University, Montreal, CA. Retrieved 2024-02-13 from https://www. priv. gc. ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2022-2023/p_202223_11.

[6] Gajula, S. (2024). *Cybersecurity risk prediction using graph neural networks*. Journal of Information Systems Engineering and Management, 9(4S), 3301–3315. https://jisem-journal.com/.

[7] Chavan, S. A., Goasvi, N. S., Khairnar, J. R., & Kapse, P. S. (2023). Mobile activity monitoring system using Android spy. *International Journal of Innovative Research in Multidisciplinary Physical Sciences*, *11*(3), 1–6. https://www.ijirmps.org

[8] Qabalin, M. K., Naser, M., & Alkasassbeh, M. (2022). Android spyware detection using machine learning: A novel dataset. *Sensors*, *22*(15), Article 5765. https://doi.org/10.3390/s22155765

[9] Soni, H., Arora, P., & Rajeswari, D. (2020, July). Malicious application detection in android using machine learning. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0846-0848). IEEE.

[10] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., ... & Ristenpart, T. (2018, May). The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 441-458). IEEE.

[11] Salih, H. M., & Mohammed, M. S. (2020, April). Spyware injection in android using fake application. In *2020 International Conference on Computer Science and Software Engineering (CSASE)* (pp. 100-105). IEEE.

[12] Mohammed, S., & Zargari, S. (2023, October). Comprehensive Analysis of mSpy Within Covert Operations. In *International Conference on Global Security, Safety, and Sustainability* (pp. 383-421). Cham: Springer Nature Switzerland.

[13] Saad, M. H., Serageldin, A., & Salama, G. I. (2015, November). Android spyware disease and medication. In *2015 second international conference on information security and cyber forensics (InfoSec)* (pp. 118-125). IEEE.

[14] Anwar, Z., & Khan, W. A. (2015). Guess who is listening in to the board meeting: On the use of mobile device applications as roving spy bugs. *Security and Communication Networks*, *8*, 2813–2825. https://doi.org/10.1002/sec.1205

[15] The Constitution of India,1950, Article 21.

[16] The Information Technology Act, Section 66(E)

[17] The Digital Personal Data Protection Act