OPEN ACCESS

International Journal Of Modern Engineering Research (IJMER)

Armordroid: Providing Privacy Protection Over Smartphone Malware Application

R.Deepika[1] H.Farhana[2] R.Sree Gowri[3] Mrs.R.Sudha M.E.., (Guide)[4]

[123],B.TECH (IT) Final Year-Arasu Engineering College, Kumbakonam, India.

[4]Assistant Professor –IT Arasu Engineering College, Kumbakonam, India.

ABSTRACT: *In the ultimate year, malicious software for Smartphone's has risen rapidly. Vendor promoters effort that has turn into more and more complicated, because of facing the demand of protecting their software free from malicious apps. Leading Approach is increasingly used by malicious software explorer to trap malware disclosure mechanisms which made the developer more complex. Specific performance frequently noticed in modern malware that fixed reasoning mechanisms are ignored and the malware instance consists of covering and complicating modules including malicious functionality in locale. In our proposed system, we represent malware detection and privacy protection over malware applications, an energetic resolution approach for identifying those malicious software components shared as pieces of an application platform. The main objective of our apps is to provide enable/disable mechanism for privacy data and provide privacy lock for user information and also to detect malware attack on any way. A number of alterations have been exactly inserted into the current trending apps which contains malicious mechanisms are invisible to trap malware disclosure techniques. Documentation is prepared for visible changes in terms of activities that arise in the modified apps and the appearing divergent indication is evaluated through an arrangement-paired system directed by the rules. It describes various numbers of covered functionalities with arrangements found in the indication. A complete explanation and a characterization of the expected model are contributed. The expanded testing results were obtained and the malware instance supports the aspect and growth of our scenario.*

Index Terms*-Malware detection, Mobile Computing, Disable/Enable user data, Privacy lock, Android.*

I. INTRODUCTION:

The representation of Smartphone for safeguard and confidentiality concerns are the major consistent dangerous than these actual in universal computing surrounding. The platform of Smartphone platforms are provided with various sensors that can regulate user locality, signal, movement and another substantial activities, name to a few. The device could be efficiently revealed the reactive portion of information because of malware locate on the Smartphone. Even to all appearance, controllable efficiency has rapidly turned into a potential threat. The source of problem in security is to accurately the capability to integrate the third-party operations from accessible markets. At the market level, safety measures level incorporate an essential configuration of protection. An improvement technology to carry out by the several market engineers to tolerate a part of configuration security verification. Authenticated details about corresponding revisions keep on remote, but the consistent latency of malware in various markets and modern analysis investigation suggest that operators cannot allow to satisfy an comprehensive analysis over various app submitted for charge to the general universal. This is another difficult by these case that determinative which operation are malicious and that aren't remains a dangerous challenge,and but that contain a risk to the user safeguard and confidentiality. The overview and contribution of this paper is to describe the Armordroid, a tool for detecting malware through malware detection signature and also to provide privacy information protection by using Disable/Enable mechanism and privacy lock.

II. RELATED WORK:

The malware are termed as malicious software package that's designed precisely to focus on a mobile device system, Such as a tablet or Smartphone to harm or spoil the device. Personal information stored on the devices are stealed by the malicious user and they control the device remotely .Malware enter into the system by downloading files from the internet and by different media. The speed of the malware today is global phenomenon by means of global communication. Today's malware is capable of doing several things, such as: stealing and sending the contact list and alternative data, protection the device entirely, giving remote access to criminals, sending SMS and MMS messages etc. Mobile malware causes severe public concern because the population of mobile phones is way larger than the population of PCs.

MALWARE DETECTION: The task of detecting malware may be classified into analysis, classification, detection and ultimate containment of malware. Several classification techniques are utilized in order to classify malware consistent with their instances and this has created it potential to acknowledge the kind and activities of a malware and new variant . Analysis of malware needs to do with identifying the instances of malware by totally different classification schemes using the attributes of famous malware characteristics. Malware detection must do with the fast detection and validation of any instance of malware so as to prevent any harm to the system. The last a part of the task is containment of the malware, that involves effort at stopping increase and preventing any damages to the system. An advertisement antivirus uses signature primarily based technique wherever the information should be frequently updated so as to possess the most recent virus information detection mechanisms. However, the zero-day malicious exploit malware can't be detected by antivirus, supported signature-based scanner, however the employment of statistical binary content analysis of file to find abnormal file segments.

SIGNATURE BASED DETECTION: signature-based detection works by checking the contents of pc files and cross-referencing their contents with the “code signatures” happiness to famous viruses. A library of familiar code signatures is updated and rested constantly by the anti-virus software package marketer. If a infective agent signature is detected, the software package acts to shield the user’s system from harm. suspected files are generally isolated and/or encrypted so as to render them inoperable and useless. Clearly there'll forever be new and rising viruses with their own distinctive code signatures. thus once more, the anti-virus software package marketer works perpetually to assess and assimilate new signature-based detection knowledge because it becomes offered, usually in real time so updates may be pushed bent users instantly and zero-day vulnerabilities may be avoided. A pattern-marching approach commercial antivirus is an example of signature based mostly malware detection wherever the scanner scans for a sequence of computer memory unit at intervals a program code to spot and report a malicious code. This approach to malware detection adopts a syntactical level of code directions so as to detect malware by analyzing the code throughout program compilation. this system sometimes covers complete program code and at intervals a brief amount of your time. However, this technique has limitation by ignoring the semantics of directions, that permits malware obfuscation throughout the program’s run-time.

DESIGN:

Armordroid is designed to provide protection over Smartphone application malware and also provide protection to privacy information. The main objective of this app is to provide protection for privacy information through Disable/Enable mechanism and also to detect malware from apps, mail and sms.

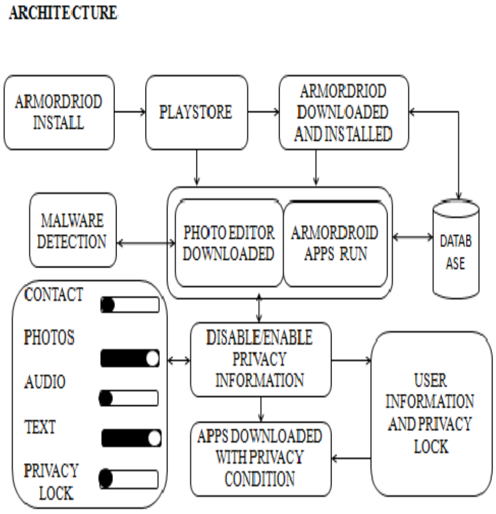


Figure: 1 Architecture of Armordroid.

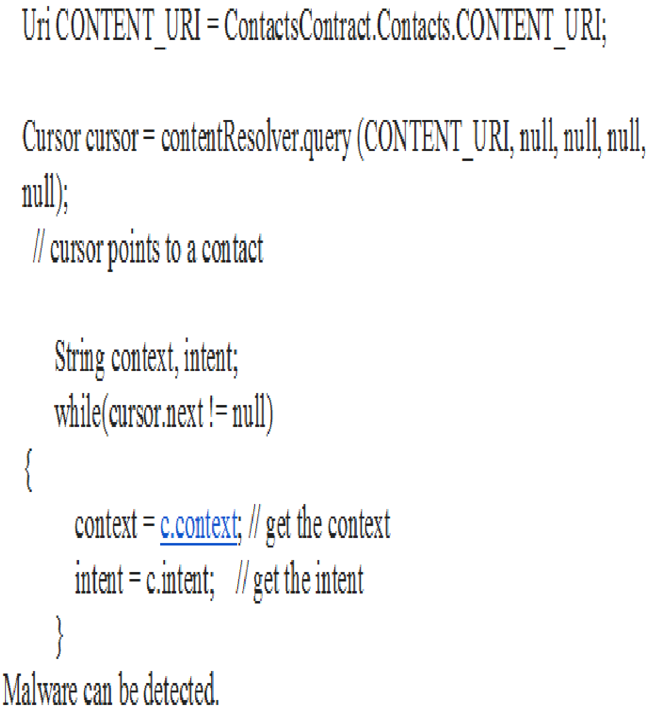
The figure 1 shows the overall architecture of the Armordroid app. The Armordroid apps are first installed from the playstore after that malware detection module is always in active stage to detect malware. After installing this app further user want to install some new app such as line app from the playstore. When downloading line app simultaneously Armordroid app is also run to detect malware and privacy conditions given in app. After that Disable/Enable mechanism is provided by the user to Enable/Disable user information to permit antagonist to access or permit user information. The information is protected by giving disable mechanism when the user information is not mandatory to provide user information for such condition app user information is disabled and run the apps successfully. Suppose some app condition is to give user information is mandatory means user can enable the needed information and go for privacy lock to provide protection for the permitted user privacy information. Thus the app can provide protection for the user privacy information.

SYSTEM MODELS:

1. Malware Detection.
2. Disable/Enable data.
3. Disable/Enable privacy lock
4. Antagonist side
5. User side

MALWARE DETECTION:

In this module malware detection mechanism is provided. The initial stage of the Armordroid apps is to check whether any malware can be occurred on the inputs of the device such as through mail, sms, and apps and so on. Once when Armordroid apps are installed on our device means malware detection can be always in active stage for detecting malware. In the case of malware available in apps that user want to install means this module cannot allow the user to install this apps, it block the apps. Malware detection signature technique is used to detect and block the malware.



```
Uri CONTENT_URI = ContactsContract.Contacts.CONTENT_URI;

Cursor cursor = contentResolver.query (CONTENT_URI, null, null, null,
null);
 // cursor points to a contact

   String context, intent;
   while(cursor.next != null)
{
     context = c.context; // get the context
     intent = c.intent;   // get the intent
   }
Malware can be detected.
```

Pseudo code for Malware Detection

Signature-based technique compares hashes (signatures) of files on a system to a list of known malicious files. It also looks among files to search out signatures of malicious code. In detection signatures, the technique includes a predefined information of notable signatures and therefore whereas scanning, it creates the suitable signature for every file (using MD5 or different hashes) and compares them with the predefined list. If they match, the file is treated as a 'threat’.

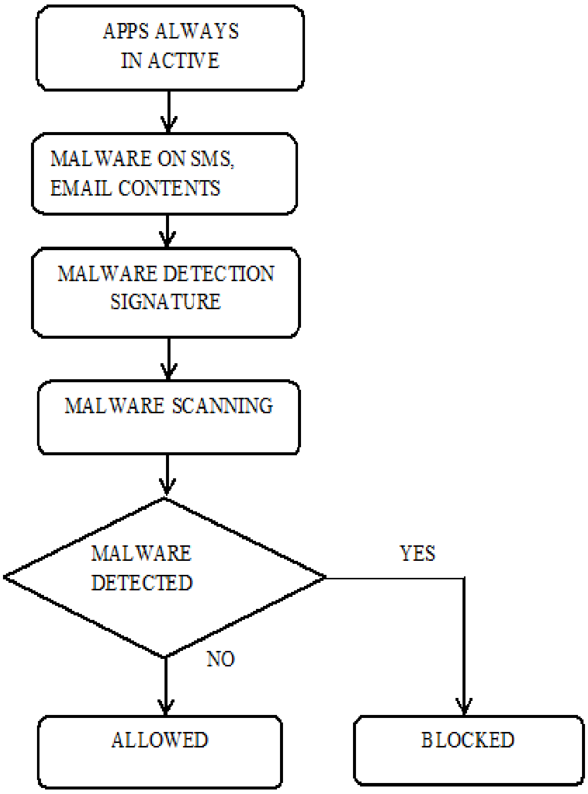
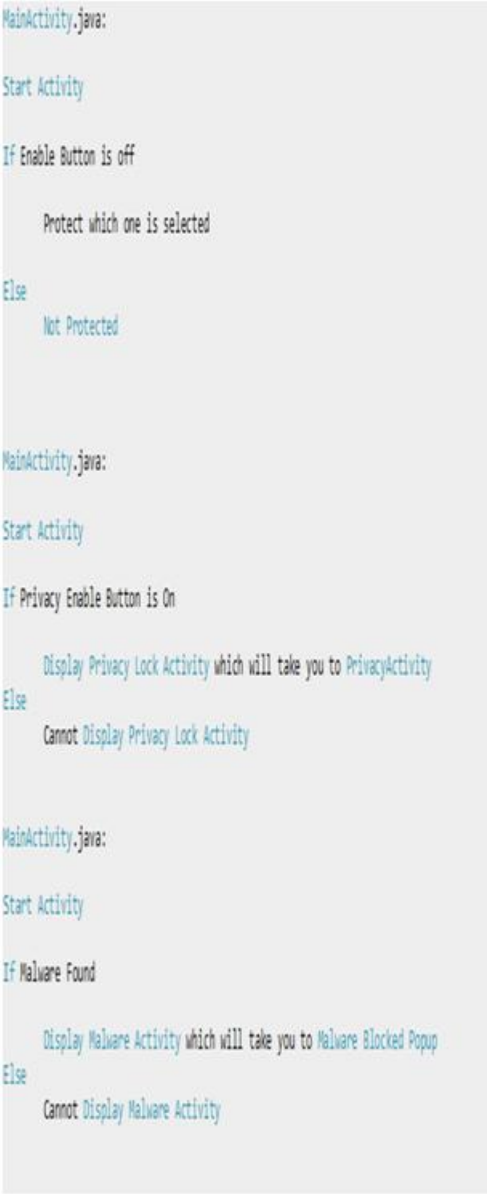


Figure: 2 Malware detection module process

DISABLE/ENABLE DATA:

In this module privacy information is protected by using enable/disable mechanism. In order to provide protection over accessing privacy information without user permission this module is developed. Whenever a new app is going to put in from the playstore and putting in news apps at the same time Armordroid apps can run and check covered condition to access privacy information..



```
MainActivity.java:

Start Activity

If Enable Button is off

    Protect which one is selected

Else
    Not Protected



MainActivity.java:

Start Activity

If Privacy Enable Button is On

    Display Privacy Lock Activity which will take you to PrivacyActivity
Else
    Cannot Display Privacy Lock Activity


MainActivity.java:

Start Activity

If Malware Found

    Display Malware Activity which will take you to Malware Blocked Popup
Else
    Cannot Display Malware Activity
```

Pseudo code for Disable/Enable data

The antagonist can access the user information only when user can provide enable service for the privacy information.If the user is giving disable mechanism means that privacy data isn't accessed by the antagonist.hen the information is protected and the new app can be run normally.

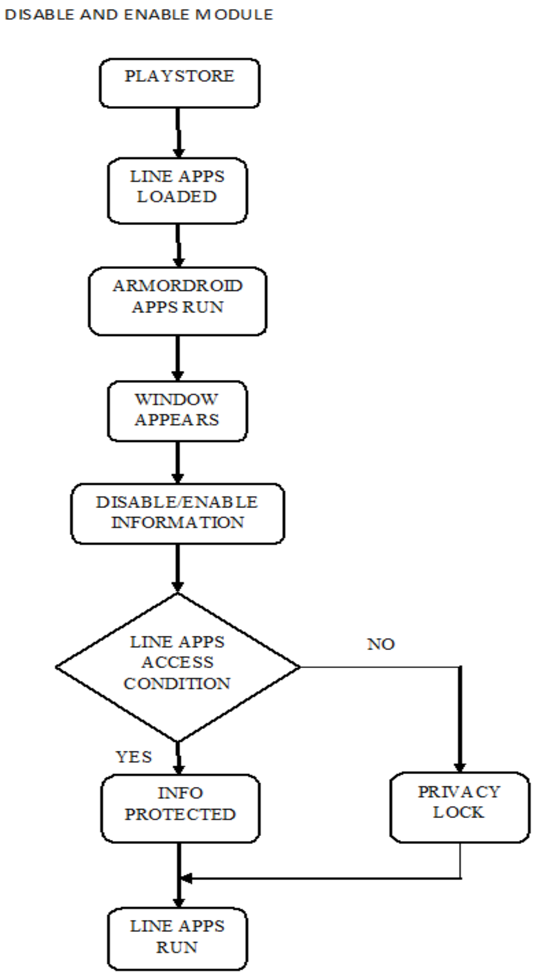


Figure: 3 Disable/Enable data module process

DISABLE/ENABLE PRIVACY LOCK

In this module requested privacy information by the antagonist is given and provides privacy lock in order to protect privacy information by some protocols. Privacy lock is an optional one in which suppose antagonist needs our information to run the application means we go for enabling privacy lock. Privacy lock is provided based on some on conditions that can two phases such as user side and antagonist side.

An antagonist is a group of institution, or concept that stands in or represents opposition against which the protagonist(s) must content. In other words, an antagonist is a person or a group of people who opposes a protocol.

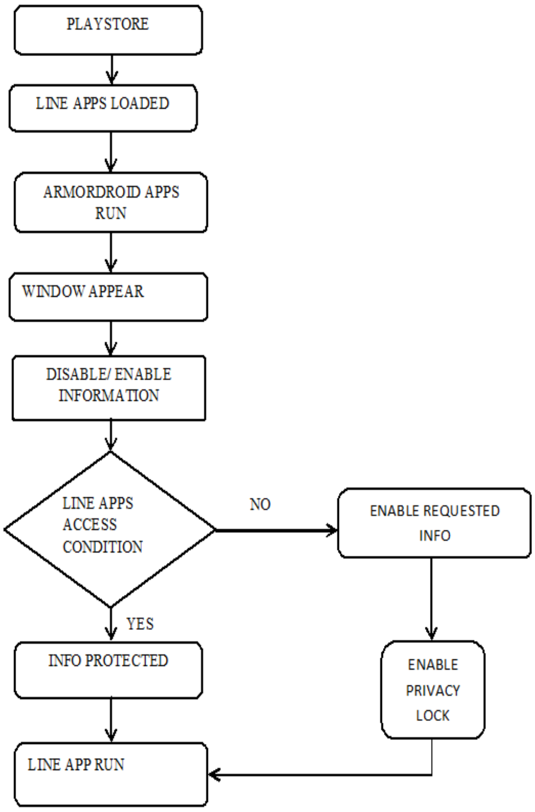


Figure: 4 Disable/Enable privacy lock module process

ANTAGONIST AND USER SIDE:

In this module the user send request to the antagonist about the information such as mail id, name, id proof etc., the antagonist has to provide this information and submit it to the user. The user verifies the information provided by the antagonist. The antagonist information is stored in the database and it is displayed to the user. If the information given by the antagonist is satisfied then the user provides access permission to access user privacy data.

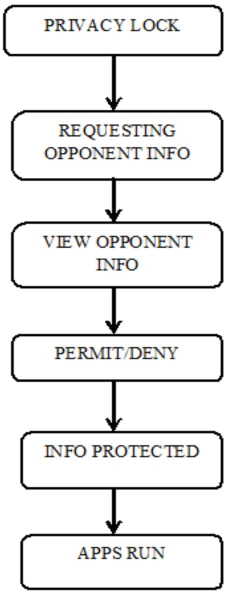


Figure: 5 Antagonist and user side module process

III. CONCLUSION:

In this paper we have presented ARMORDROID, a framework for malware detection and providing protection for user privacy data by using a malware detection signature. We have described its architecture and provide Pseudocode for malware detection. Malware detection signature technique that can identify malicious components hidden in the apps and it provide privacy for user data through Disable/Enable mechanism. Additionally we provide privacy lock for user personal information. In future we extend this by using a Hybrid Signature-based Detection for malware detection. We can update this project by verifying id proof in the respected server automatically and privacy information can be provided based on confidential and non-confidential data's.

References:

[1]. G. Suarez-Tangil, J. E. Tapiador, P. Peris, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices,"IEEE Comms. Surveys & Tut., vol. 16, no. 2, pp. 961–987, May 2014.

[2]. C. Zheng, S. Zhu, S. Dai, G. Gu, X. Gong, X. Han, and W. Zou, "Smartdroid: an automatic system for revealing UI-based trigger conditions in Android applications," in Proc. ACM, ser. SPSM '12.New York, NY, USA: ACM, 2012, pp. 93–104.

[3]. M. Zheng, M. Sun, and J. C. Lui, "Droidray: A security evaluation system for customized android firmware," in Proc. ACM, ser.ASIA CCS '14. New York, NY, USA: ACM, 2014, pp. 471–482.

[4]. V. Rastogi, Y. Chen, and W. Enck, "Appsplayground: automatic security analysis of smartphone applications," in Proc. ACM, ser.CODASPY '13. New York, NY, USA: ACM, 2013, pp. 209–220.

[5]. Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in Proc. IEEE, ser. SP '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 95–109.

[6]. G. Suarez-Tangil, J. E. Tapiador, and P. Peris-Lopez, "Stegomalware: Playing hide and seek with malicious components in Smartphone apps," in INSCRYPT 2014, December 2014.

[7]. M. Grace, Y. Zhou, Q. Zhang, S. Zou and X.Jiang, "Riskranker: scalable and accurate zero-day Android malware detection," in*Proc.*, ser. MobiSys '12. ACM, 2012, pp. 281–294.

[8]. W. Enck, P. Gilbert, B.-G. Chun, and al., "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," in *Proc. USENIX*, ser. OSDI'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6.

[9]. R. Hasan, N. Saxena, T. Haleviz, S. Zawoad, and D. Rinehart, "Sensing-enabled channels for hard-to-detect command and control of mobile devices," in *Proc. ACM SIGSAC*, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 469–480.

[10]. Y. Wang, K. Streff, and S. Raman, "Smartphone security challenges," IEEE Computer, vol. 45, no. 12, pp. 52–58, 2012.

[11]. A. Desnos and et al., "Androguard: Reverse engineering, malware and goodware analysis of android applications," https://code. google.com/p/androguard/, Visited Feb.2015.

[12]. G. Suarez-Tangil, F. Lombardi, J. E. Tapiador, and R. Di Pietro,"Thwarting obfuscated malware via differential fault analysis,"*IEEE Computer*, vol. 47, no. 6, pp. 24–31, June 2014.

[13]. R. Hasan, N. Saxena, T. Haleviz, S. Zawoad, and D. Rinehart,"Sensing-enabled channels for hard-to-detect command and control of mobile devices," in *Proc. ACM SIGSAC*, ser. ASIA CCS '13.New York, NY, USA: ACM, 2013, pp. 469–480.

[14]. K. Tam, S. J. Khan, A. Fattori, and L. Cavallaro, "Copperdroid: Automatic reconstruction of android malware behaviors," in *NDSS Symp*. Internet Society, February 2015.

[15]. S. Schrittwieser, S. Katzenbeisser, P. Kieseberg, M. Huber, M. Leithner, M. Mulazzani, and E. Weippl, "Covert computation: hiding code in code for obfuscation purposes," in *Proc. 8th ACM SIGSAC*, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 529–534.

PROFILE:

Mrs.R.SUDHA M.E working as Assistant Professor in Arasu Engineering College approved by AICTE and Anna University Chennai. She was vast experience in Computer science Engineering.

Miss.R.DEEPIKA is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Networking and Mobile computing.

Miss.H.FARHANA is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Database Management and system and Mobile computing.

Miss.R.SREE GOWRI is a student of **B.TECH (IT)** at Arasu Engineering College approved by AICTE and Anna University Chennai. Her areas of interest are Networking and Mobile computing.