STUDY ON PERFORMANCE ISSUES IN MOBILE APPLICATION
Prerna Kumari, Prasenjeet Bhadra, G.Ramya
School of Information Technology and Engineering, Vellore Institute of Technology, Vellore-Tamilnadu, India
Email: engr_ramyaa@yahoo.com
Received on 25-10-2016
Accepted on 02-11-2016

Abstract
This paper provides an overview of performance issues related to mobile applications. As development of applications that run on mobile devices requires lot of resources and lead to wide area of performance issues. Among which the main categories are user interface design, application portability, quality, and security. Versatile program based application execution is generally intensely reliant on system and server application execution. The execution is typically slower thus and prompts a lessened client experience based on performance issues such as slow working, excessive memory and net usage, security problem etc. Also, a few applications may have higher execution than others as there is no standard.

Keywords: Application Crash, Application log, Amoled screen, Ransomware.

Introduction
Industry analyzers evaluate that there are more than 250,000 applications accessible through the different mobile stores and other devices, some of which are accessible for various sorts of gadgets. A large portion of the applications were generally little, averaging a few thousand lines of source code, with maybe a couple engineers in charge of imagining, outlining, and actualizing the application, there was a sharp divide between “native” applications, those that run entirely on the mobile device and web applications, which includes a little gadget construct customer with execution happening in light of a remote server. Furthermore, the designers have no clue how the applications are performing, what clients are doing with them, or truly anything aside from the intermittent crash report [1]. One composition applications for the cellular phone needs to remember memory use, as they are not allowed to devour loads of stack as they would be for a Java application running on goliath application server. Phones and tablets does not have a long battery life. Short battery life is particularly an issue for phones whose battery is littler than the tabletbased client with execution occurring on a remote server... A mobile device app needs to be properly written, so
that it does not use up the limited memory on the phone or run down the battery too fast. The programmer needs to know how to stop threads running in the background, how to destroy variables or save data, and the correct time to take each action. For example, when the app has lost focus it has switched to the stopped status. Mobile apps often crash: even Chrome, Twitter, and Netflix. Early versions of Firefox on Android crashed a lot too [2]. When an app is down, by definition that is a performance hit. Mobile apps security deals with preventing Data Theft and Leakage and Restricting High-Risk Access & Transactions, so how we secure the mobile work force we will discuss further in paper, can apps be realistically secure app on creation, particularly on a first round? Probably no. However, you can focus on these trouble sources and do your best to create strong authentication, validation, exception handling for the things that can and will go right, thus let’s leads to mobile crash. A mobile crash is the sudden disappointment of an application shutdown or working framework failure. The four module which we will discuss further in paper according to performance issues of mobile are –Application crash, Security, Battery life and Storage issue.

Application Crash

With the increase of the installation of native and web based apps, with minimum number of hardware specification mobile system tends to crash for which it leads to lag, system crash, memory dump and many other problems. With high specification, the mobile systems are eligible to handle bigger application in terms of storage and resource allocation but it also increases the rate of the minimum rate of temperature for which it is unable to cope up and leads to battery related problems. In our paper, we have mentioned about the application crash and bug report which comprises two things that is generating the bug report/crash report and posting it to the developer for applying functionalities through manipulations. The developer will than release the updates based on the beta version of the application stage by stage in collecting the report of each crash until the application that is installed in the mobile system works perfectly and smoothly. In today industry, portable devices are getting used and used by millions of

Figure 1: System architecture.
people where smartphones plays a major role. With increase in the rapid use of this device, installation of application is also getting bigger and bigger even the storage incorporated in the system is not enough. Certain use of the applications rapidly increases the memory consumption for which all the resources that were available for system use are than allocated to application level hence leading to a shortage of memory. Somehow both the system program and application level programs are unable to incorporate with the resources provided by the manufacturers that leads to the occurrence of deadlock. This is a major issue in the mobile system dominated technology where each and every applications are getting smaller and smaller in size and are incorporated in a single system where it is expected to run at its utmost level. Based on the concurrency, simultaneous, and attractive user interfaces, all the applications are getting a wider view on the objects surrounded to different stake holders but as the device is smaller as compared to PC systems, someway it cannot go beyond its limitations which thus lead to application crash and bug report generation that is used by the developers for agile development and its modification.

Figure 2. Crashes per App Launch: iOS and Android [17]

Depending on the proliferation on IOS and android operating system, the number of the application crash is increased drastically. There are steps on which the developers of the most popular software vendors are developing and testing there apps on a regular basis in a new platform versions each day but still the amount of crashes will be going on because there is no stable platform to test the new applications which are developed for upcoming version of mobile operating systems[9].The present stimulators and platforms are only incorporated with the development of apps that can only be used with the existing operating systems.

Figure 3. Mobile system architecture.
Security

Brilliant cell phones (Smartphones and tablet PCs running versatile working frameworks) have changed the path in which we make and devour advanced data and seldom leave our sides. They have, and are keeping on supplanting, other purchaser advanced hardware including PCs, portable workstations and note pads, TVs, gaming gadgets/supports, satellite route gadgets and individual music players. In addition to security dangers a mix of expanding Smartphone possession and the utilization of more significant information administrations on these gadgets has prompted Smartphones turning into a more alluring focus for fake and unlawful activities. Malware is a case of how a defenselessness is abused, making code that adventures shortcomings and bugs, in the Operating System for pernicious purposes – to concentrate individual data or to sanction money related misrepresentation on the Smartphone proprietor. This is the reason it is basic to have a powerful and proficient Smartphone Operating System programming overhaul handle that finds vulnerabilities before the awful folks do, fixes them and after that pushes the resultant programming redesign to all influenced Smartphone proprietors before the defenselessness can be generally misused. As a portion of the cell phone working framework merchants are making a conventional showing with regards to by discharging upgrades and fixes so that after its fuse with the cell phones in application level it can play out its essential powerlessness component to improve and enhance the security system of the to a great extent utilized compact gadgets[7]. A portion of the merchants have proposed numerous dangers taking care of strategies, for example, fig 1 demonstrates the upgrade procedure of the cell phone weakness redesigns therefore killing the reason for any deceitfulness and information rupture yet at the same time there is a reason of fracture in versatile working framework for which 1 million of android clients will be influenced from these issue. Thus reducing these will include.

A. Secure the Code: Building a Secure Application

Portable malware regularly taps vulnerabilities or bugs in the configuration and coding of the versatile applications they target. Late research from Kind sight reported by Info security demonstrates that noxious code is tainting more than 11.6 million cell phones at any given time, and the quantity of portable malware tests is developing at a quick clasp, expanding by twentyfold in 2013. Indeed, even before a weakness is abused, aggressors can acquire an open duplicate of an application and figure out it. Prominent applications are repackaged into "maverick applications" containing malignant code and are posted on outsider application stores to bait and trap clueless clients to introduce them and trade off their gadgets. Endeavors ought to search for apparatuses to help their designers to recognize and
close security vulnerabilities and afterward solidify their applications against figuring out and altering. To that as it may, "customer applications" still to encounters a risk as if they may not experience the suitable solidifying process; and if rebel applications, malware and venture applications have the same gadget, the danger is unmistakable.

b. Secure the Device: Detecting Compromised and Vulnerable Run-Time Environment As secure as an application seems to be, its security depends on the hidden gadget's security. Jail broken or established gadgets or the nearness of rebel applications can speak to an execution hazard that might be took into consideration certain undertaking applications yet not for others. Undertakings ought to investigate approaches to powerfully gage the security of the fundamental gadget. In the first place, the portable application sandbox, which is pervasive in present day versatile working framework plan, must be in place. Establishing or jail breaking the gadget breaks the basic security model, and it is exceptionally prescribed to confine these gadgets from getting to big business information. Besides, escape innovation is advancing quickly to avoid location; adapting to these instruments is vital to staying aware of these dangers. Versatile malware doesn't generally depend on the gadget being jail broken, be that as it may. Over the top utilization of authorizations to the versatile applications — which are allowed by the client, frequently of course — can give malware and maverick applications access to essential administrations (e.g., SMS) used to encourage deceitful exercises. Endeavors ought to consider up and coming knowledge sources and application notoriety administrations to track the tsunami of uses — and their related danger — as they enter versatile application stores once a day. Utilizing this information, application abilities could be empowered or handicapped in view of the gadget hazard profile.

c. Secure the Data: Preventing Data Theft and Leakage

At the point when portable applications access venture information, records and unstructured data are regularly put away on the gadget. On the off chance that the gadget is lost or when information is imparted to no enterprise applications, the potential for information misfortune is elevated. Numerous ventures are now investigating "remote wipe" capacities to address stolen or lost gadgets.

Portable information encryption can be utilized to secure information inside the application sandbox against malware and different types of criminal access. To control application information sharing on the gadget, singular information components ought to be encoded and controlled.

d. Secure the Transaction: Controlling the Execution of High-Risk Mobile Transactions. Since versatile applications empower clients to execute with big business administrations on the go, the danger resistance for exchanges will
change. For instance, perusing HR-related substance might be regarded generally safe versus the endorsement of an expansive installment to another supplier.

Associations ought to adjust a methodology of danger mindful exchange execution that limits customer side usefulness taking into account arrangements that consider portable danger variables, for example, gadget security qualities, client area, and the security of the system association, among others. Notwithstanding when customer side exchanges are permitted, undertaking applications can influence a venture portable danger motor to correspond hazard variables, for example, IP speed — access to the same record from two areas that are far separated over a brief period — client access examples and information access profiles. This methodology extends the undertaking's capacity to identify and react to complex assaults that can traverse numerous association channels and apparently random security occasions.

Securing Enterprise Mobile Applications Against Evolving Threats: IDC expects that almost 69 percent of all cell phones utilized for business are possessed by the workers as opposed to the venture. These cell phones are turning out to be more alluring focuses for malware journalists that are simply taking after the cash. BYOD development rates increment the danger of individual gadgets contaminating endeavor systems. To secure the portable workforce in the period of BYOD, IT security experts and line-of-business officials must consider how portability impacts their business hazard profile.

The proposed structure takes a gander at the gadget, the information, the application and the exchange as segments of a solitary continuum that must be secured to minimize the business hazard connected with portability; it's about finding a harmony amongst convenience and relieving hazard. The proper versatile security system will empower undertakings to procure the profitability picks up and improve worker fulfillment while restricting the introduction to their basic data and business resources. Some of the vendors have proposed many threats handling tactics such as the update process of the smartphone vulnerability updates thus eliminating the cause of any fraudulence and data breach but still there is a reason of fragmentation in mobile operating system for which 1 million of android users will be affected from these issue.

As per Intel analytics, major security threats are arising out of the developing industry with the final product which is incurring a huge loss on the mobile systems. As one of the virus called ransomware is widely affecting the performance of mobile system by exploiting its access controls and giving permission to its third party vendors. Here in fig 4, states the system how it is effecting the performance on a quarterly basis by popular ran some ware virus.
Some of the policies and strategies proposed to cope with this threat are:

- Backing up of data.
- Perform an ongoing user-awareness education.
- Blocking of unwanted or unneeded programs and traffic.
- Keeping of the system patches up to date.
- Protect endpoints and employ antispam.

At this point of view, with this preventing mechanism, we can lessen the number of potential threats arising in the mobile ecosystem which are widely affecting the performance as well as the user experience.

**Battery Life**

Initially, some foundation: most cell phones have either a lithium-particle battery or a lithium-polymer battery [3]. Both are really lithium-particle however, and in that capacity, don't have a 'memory', which implies you can charge them from any level – you don't need to completely release them before energizing them – and you don't need to charge every one of them the best approach to 100 percent. Truth be told, these sorts of batteries experience the ill effects of low voltage issues, so it's quite to in part charge them say, from 20 percent to 90 percent than to completely charge and completely deplete them.

Fundamental battery cleanliness –

Keep your phone cool -As indicated by the Battery University blog by Cadex Electronics, telephone batteries corrupt much speedier when they're hot, whether you're utilizing the telephone or it's unmoving. Abstain from leaving your phone on the dashboard of your auto on a sunny day.
Charge somewhere around 40% and 80% - The most ideal approach to keep up cell phone batteries is to keep your telephone battery more than 40% charged. Always permitting the battery to go from totally full to totally purge can harm it and decline its ability after some time. On the other side, leaving your phone connected to when it's totally full can likewise debase the battery. Best practice? Keep your battery somewhere around 40% and 80% charged.

Periodically let your battery pass on -Battery University proposes that adjustment – completely releasing then energizing your telephone's battery – once like clockwork helps it keep up its charge limit.

Continuously download upgrades -Whether upgrades are expected for downloaded applications or so updates itself, they for the most part incorporate bug fixes and changes that enhance execution, including how effectively battery is utilized.

Dark backdrop can expand battery- On the off chance that your telephone has an AMOLED screen (like most Samsung gadgets), utilize a dull hued foundation [4]. Dark backdrop can expand battery life in light of the fact that AMOLED screens just enlighten the hued pixels. Dull pixels are faint, so the more dim pixels you have, or the darker pixels, the less power is required to light them up.

Nap - With the passage of Marshmallow came another component called Doze, which helps you get more out of your contraption's battery. Close by Google Now on Tap, Doze is the most striking development to Marshmallow. It is enabled as is normally done and essentially allows your device to enter hibernation mode when it has been sat unused for a postponed time allotment.

Turn off Google hot words -Prevent your telephone from continually tuning in. Google's OK Google voice seeking is a phenomenal and regularly exceptionally useful component. The issue is that it can wreak destruction with your battery. Particularly on the off chance that you don't really utilize it or just utilize it every so often. Go into Google settings from your application drawer and tap Voice heading. On the following page, select OK Google discovery. In this menu, the best alternative for battery life would be to untick all the containers, however in the event that you are a devotee of OK Google, simply tick the From the Google application box to guarantee your gadget is just listening when you're in the Google application. Take after alongside the video underneath for the full procedure.

Try not to let your applications fall obsolete -Keep your applications upgraded. There's a reason designers always redesign applications, and more often than not it's for memory or battery improvement. Keeping your applications upgraded additionally implies you have the best improvements accessible. In like manner, erase old applications you no more utilize, in light of the fact that these might run foundation forms that bite up RAM and battery life.
Once you've guaranteed your applications are up and coming you can experience them separately and check on the off chance that they're improved for battery life. This should be possible rapidly. Simply go into your Settings and tap Battery. From that point hit the menu catch (three dabs at the upper right of your screen) and go to Battery streamlining. From that point you can see which applications are improved and transform them. You can just change the unnecessary framework applications. Watch the video underneath to perceive how this is finished. In like manner, you can set your telephone to quite mode when you're snoozing or utilize rest or obstructing as far as possible for what your telephone does amid specific times of the day, whether that is while you're sleeping, at work or in a meeting. Cool applications, for example, IFTTT let you make decides that can help you spare battery life as well.

You don't should be associated all day, every day -Turn off GPS, Bluetooth, NFC, Wi-Fi and portable information at whatever point you needn't bother with them. Killing area information, or changing your area settings to utilize Wi-Fi or 3G information instead of GPS works impeccably well. This will expand battery on your Android gadget. Just turn on Bluetooth and NFC the length of you need them (despite the fact that they expend almost no force), and there's no need both. Wi-Fi and portable information turned on at all times, particularly on the off chance that you know precisely when you'll need either. On the off chance that you utilize Wi-Fi a great deal however, say at home and at work, then it bodes well to keep set your Wi-Fi to 'Dependably on amid rest' as this uses less power than to have your Wi-Fi reconnecting each time you wake your telephone. The greater part of these can be found in your Quick settings. Try not to get impeded by gadgets -Trench gadgets you don't require, particularly those associated with the web, for example, climate gadgets. In the event that you have numerous gadgets over a few home screens, which are continually matching up and redesigning (Twitter, reddit, climate, Gmail and so forth), you're not helping your battery. Simply hit the applications when you require them. In the event that you as of now have a group of futile gadgets on your gadget then you simply need to do a few things and they'll be no more. Long push on a clear space on your home screen. Presently drag the gadget you don't require into the garbage canister at the top or base of your screen (it relies on upon the brand). Investigate the battery sparing elements on your phone -All ROMs, whether stock Android, OEM UIs, for example, Touch Wiz, or custom ROMs like Cyanogen Mod, have different settings in the menu to preserve or advance battery utilization. HTC has Extreme Power Saving Mode, Samsung has Ultra Power Saving Mode, Sony has STAMINA mode. Locate these different choices for your gadget and ROM and make them work for you. Regardless of the possibility that your telephone doesn't have layers of battery sparing components like a few (or you just don't need cripple such a large number of elements), in any event make utilization of the essential
Try not to fall into the auto-sync trap - Turn off auto-matching up for Google accounts. On the off chance that you needn't bother with each and every Google account redesigned at regular intervals, simply go into Settings and Google record and kill auto-sync for those applications you don't require continually upgraded.

Some applications – like email – let you physically invigorate when you dispatch them, instead of running different auto-revives for the duration of the day when you may not require them to. The same goes for Twitter, Reddit and co. unless you require consistent overhauls or push warnings (like for Facebook or your date-book) simply match up when you really utilize the application.

Clients: If you have various client accounts set up on your Android telephone or tablet, you'll see a different "Client" thing for every client here. This helps you see how much other client accounts added to your battery utilization. Hence phone unmoving or Tablet sit: Your Android gadget utilizes some measure of force since it's on, regardless of the fact that it's totally sit still in a low-control state.

Storage

Storage in mobile apps at the point when building versatile applications you will regularly need to store tireless information on the gadget itself. This kind of capacity permits your applications to work successfully when there is no association and additionally offering more progressed and frequently quicker usefulness than server side stockpiling as it were. Much of the time your application may have both customer side stockpiling and server side stockpiling and your application will deal with the stream of information between the customer and server. Application Craft gives every one of the apparatuses you have. The accompanying customer side stockpiling strategies are accessible to you, all of which are standard HTML5 highlights however not as a matter of course upheld in all programs. Perused on to get the abominable.

![Storage Architecture](image-url)

**Figure 5. Storage Architecture [19].**
Cookies
This is the most essential approach and is extremely restricting as you can just store 4KB of information in a treat. It is likewise defenseless against being erased if a client just clears treats. It is suggested just for the most straightforward stockpiling necessities and for Web Apps. Neighborhood Storage has the same level of effortlessness yet significantly more stockpiling and more dependable in Native Apps. Application Craft gives the app.cookie() technique for setting and getting treats [8].

Local Storage
This is the most ideal approach to store steady information for applications that don't require social database capacities. It takes into account quick stockpiling of information and is truly simple to utilize. You can take your JavaScript questions and clusters and essentially change over them into JSON utilizing JSON.stringify() and you can simply store it with a straightforward order. Reestablishing information from Local Storage is generally as simple. You basically get your information with a solitary call and after that utilization JSON.parse() to change over your JSON string again into a JavaScript question or exhibit. Nearby Storage has a 5MB point of confinement for each area for typical web applications. Be that as it may, can now surpass this farthest point in the event that you convey your App utilizing our single tick Phone Gap/Cordova choice where as far as possible is 25MB.
Cautioning: iOS 5.0.1 has an awful bug that implies that iOS can erase your whole Local Storage information as a piece of its cleanup operations when it needs to make space. Neighborhood Storage should be determined. This bug has now been altered in iOS 6 yet you ought to know about this danger. You won't not see, but rather on the off chance that you can't go for broke, notice the notice and look to Phone Gap + SQLite arrangement.

WEB SQL FOR PURE WEB APPS
This is somewhat of an issue tyke. Web SQL utilizes the capable SQL Lite motor to give full social database capacities. For anybody acquainted with MySQL, Postgres, and SQL-Server and so on, this is successfully what you are getting. The main downside is that for some unprecedented reason Mozilla have chosen in their definitive shrewdness that they would prefer not to bolster it and it has in this way been belittled as a formal HTML5 standard. Practically speaking, however, it is still completely accessible for versatile applications as Web kit (and numerous different programs) still completely underpins it. In any case, building up a vast application utilizing Web SQL is certainly a danger as a year or two down the line you could all of a sudden discover the mat hauled out from under your feet. Be that as it may, there is some uplifting news, so read on. Web SQL is not about as simple to use as Local
Storage, which ought to be utilized where conceivable. Web SQL databases for a given area are confined to normally 5MB (program subordinate) [8].

SQLITE FOR COMPILED APPS

On the off chance that you are utilizing AC Mobile Build to aggregate your application, then you can assemble applications utilizing SQLite. SQLite is a mainstream decision as inserted database for nearby stockpiling in local applications and with this approach the SQLite database library is a piece of your application. Likewise, there are no capacity size points of confinement [8].

INDEXED DB

This is a No SQL database execution that is certainly turning into a part of the W3C HTML5 detail yet up 'til now (July 2012) is not actualized over all programs and no versatile program presently bolsters it. Now, along these lines, there is very little worth saying in regards to it to the extent Application Craft is concerned [8].

CUSTOM DATA STORAGE OPTIONS (PHONEGAP/CORDOVA) - Since Application Craft underpins a single tick gathering of modules without the requirement for you to introduce any compilers on your desktop, any custom information stockpiling instrument that is accessible as a module can be added to the framework. With a specific end goal to keep up quality and guarantee things work appropriately, we test modules ourselves before adding them to our library of upheld modules [8].

We all know that storage is never much as to appear to be. A device with 32GB of storage, for example, will have a lot less because of the operating system and preinstalled apps, and also from the squandered space brought on by how os' arrangement the capacity medium. Most of us realize that, however regardless we get indignantly beguiled when we attempt to introduce applications or OS overhauls onto our Android or iOS gadget, just be told there's deficient room - however the redesign or application consumes far less room than what is When Android demonstrates the "Inadequate Storage Available" mistake Lack of working space is the reason for the "Deficient Storage Available" blunder that intermittently torments Android users, there are a few conceivable foundations for the absence of adequate working storage. Android applications utilize three arrangements of storage room: for the applications themselves, for the applications' information documents, and for the applications' reserve. Those reserves can develop very substantial, yet they are accounted for as free space by Android - however in reality that space is not accessible as a working space for application installation. If you get the "Deficient Storage Available" mistake, purge your
application reserve to check whether that clears up enough working space for the establishment. Instructions to do as such relies on upon what stage you are running, and also from what gadget creator.

**Conclusion**

As talked about in our paper, application crash can bring about overwhelming harm to our mobile phones by uncalled for shutdown to phone which can be quite a while issue. So to manage this issue Google Play Developer Console gives you a chance to get to crash reports. That will give you some data about the condition of your application when it went down, ideally giving you enough data on to change the code to settle that, in addition to when it crashes the client has the opportunity to give feedback. So as are we probably aware mobile applications are not secure and shielded from dangerous hackers. It’s important that back-end administrations be solidified against malevolent attacks. This implies all APIs ought to be confirmed and legitimate security strategies ought to be utilized to guarantee just approved work force have access. There are approaches to compose code to preserve memory and battery. One composition applications for the cellular telephone needs to remember memory use, as they are not allowed to devour bunches of pile refuse accumulation is done, Short battery life is particularly an issue for phones whose battery is littler than the tablet. Discharge handles to gadgets like Bluetooth and the NFC radio and communicate beneficiaries. On the off chance that you see the message ‘inadequate capacity accessible’ on your Android telephone or tablet and you do have space accessible then store of separate application ought to be cleared promptly this will oversee memory to some broaden.

**References**

2. Correl Sense, Performance issues with Android Mobile appow to store battery.,2014.
3. Battery University, How to store battery, 2016.
4. Cory Scmidt, how to save battery life on your android phone.
5. How to geek, How to see which app are draining your battery on android phone or tablet.
6. App knox, Top 5 security issues in mobile applications.
8. Tomio Geron, Do ios crash more than android app.
10. App dynamics, App dynamics Business white papers”.

12. Hewlett Packard Enterprise, Mobile load performance testing for mobile applications.


14. Kavindra Kumar Singh, Dr. Praveen Kuma.

15. Optimizing the Performance of Mobile Web Application.
